BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

AN EVALUATION OF BANK SECURITY AND FRAUD PREVENTION: A CASE STUDY OF BARCLAYS BANK ZIMBABWE. (2010-2015)

TAURAI VITALIS CHIGOVA

B1025625

SUPERVISOR: MR CHIKOMBA

SUBMITTED IN PARTIAL FULFILLMENT OF THE BACHELOR OF COMMERCE (HONOURS) DEGREE IN FINANCIAL INTELLIGENCE

March 2017

RELEASE FORM

Name of student:	Chigova Taurai V
Dissertation title:	An evaluation of Bank security and fraud prevention: case study of Barclays Bank Zimbabwe.
Degree title :	Bachelor of Commerce (honours) in Financial Intelligence
Year this degree was granted:	2017

Permission is hereby granted to Bindura University of Science Education Library to produce single copies of this dissertation and to lend or sell such copies fazzor private, scholarly or research purposes. Only the author reserves other publication rights; neither the dissertation nor extensive extracts from it may be printed or otherwise reproduced without the author's written permission.

Signed	.....
Permanent address	2 Mount Cazalet, Gwanda
Date	March 31, 2017

APPROVAL FORM

The undersigned certify that they have supervised the student **Chigova Taurai V**'s dissertation titled: **An evaluation of bank security and fraud prevention: a case study of Barclays Bank Zimbabwe,** submitted in partial fulfillment of the requirements of the Bachelor of Commerce (Honours) Degree in Financial Intelligence.

……...	……
SUPERVISOR	DATE
……..	……
CHAIRPERSON	DATE
……..	……
EXTERNAL EXAMINER	DATE

DEDICATION

I dedicate this work to my family for the support they gave throughout the academic time. Above all, I thank God for His wisdom.

ABSTRACT

This study investigated the role of bank security in fraud detection, prevention and investigation. The wave of fraud in the banking sector has been prevalent, hence the researcher felt that there is paucity of information on how to define clearly the role and extent of bank security to fraud. The research was aimed at showing the consequences of fraud in commercial banks using case study of Barclays Bank Zimbabwe. The objectives of the research were to identify different types of frauds in banks, to highlight impacts of fraud in banks and to suggest ways to combat fraud in banks. A descriptive research design was used to obtain quantitative and qualitative data. A sample of 37 respondents out of a population of 80 was used comprising of bank managers, bank tellers, accounting personnel and the human resource personnel. Random sampling technique was used in the selection of respondents in the study. Face to face interviews and questionnaires were selected as research instruments. Analysis of data was done using Microsoft excel. Data collected was presented through the use of tables, graphs and figures. The study found out that bank fraud is becoming more and more prevalent and that banks face considerable profit losses due fraud. Amongst all other preventive measures in prevention of fraud in banks, effective internal controls were found to be the most important. The study recommended that further research should be done especially on computer related crime that affects banks since development of technology provides various ways of committing more sophisticated ways of committing fraud in banks.

ACKNOWLEDGEMENTS

First of all, I would like to express my sincere appreciation to my supervisor, Mr. Chikomba who guided me throughout the research project. His constant guidance, insightful suggestions, and constructive ideas are the essential inputs and encouragement for me in order to complete this study.

Last but not least, I would like to express my gratitude and honour to the almighty God who gave me the wisdom and knowledge to undertake this project without hindrances. May his name be forever glorified.

TABLE OF CONTENTS

LIST OF TABLES

Figure **Page**

LIST OF FIGURES

Figure **Page**

CHAPTER I

INTRODUCTION

1.0 Introduction

Every public and private domain is susceptible to fraud. With regard to sheer size of other institutions, victims of some financial fraud may fail to attract sympathy as they are assumed to be wealthy and to have willingly parted with their money (Shichor et al., 2000). This research is going to look at fraud in commercial banks with reference to Barclays Bank (Pvt) Ltd, a pronounced financial institution in the commercial sector. This chapter will look at the background to the study, statement of the problem, research questions and the objectives of the study. Furthermore the researcher will look at the assumptions of the study, delimitation of the study and the significance of the study.

1.1 Background

Barclays Bank Zimbabwe (BBZ) is a commercial bank in Zimbabwe. The Bank's parent company is Barclays PLC domiciled and headquartered in London, United Kingdom. It is one of the commercial banks licensed by the Reserve Bank of Zimbabwe, the national banking regulator. The bank is a medium-sized financial services provider in Zimbabwe, serving large corporations, small-to-medium enterprises (SMEs), as well as individuals. As of December 2013, its total asset base was valued at about US$281.5 million, with shareholders' equity of US$40.5 million. In October 2011, the bank was the fifth-largest commercial bank in Zimbabwe, based on customer deposits, with a 7.1% market share.

Barclays Bank Zimbabwe was established in 1912, and has operated continuously since. As of December 2011, BBZ employed 1,022 permanent staff, in a commercial banking network of 38 branches in all large urban areas in the country. The bank's Zimbabwe Operations headquarters are located in Harare, the capital of Zimbabwe, and the largest city in that country.

This study seeks to examine bank security measures in relation to prevention, detection and investigation of the crime of fraud. Fraud negatively impacts organisations in various ways

including financial losses, reputation impairment, psychological and social implications. Findings from the American Bankers Association 2013 Deposit Account Fraud Survey revealed fraud against bank deposit accounts cost the industry $1.744 billion in losses in 2012. Debit card fraud accounted for more than half of 2012 losses (54%), followed by cheque fraud (37%). Online banking and electronic transactions conducted via wire, automated clearing house (ACH), or other means accounted for the remaining nine percent of losses.

Financial institutions in Zimbabwe have been facing a number of financial crime caused by their employees. To mention a few banks affected, Steward Bank where an employee was up for $37000 fraud (Kaseke 2014). A Banc ABC ex-employee, an international banking officer manipulated a client's account and fleeced more than 1 million through fraudulent transfers (Machakaire 2013). A plan by Stanbic employee to defraud over $28,000,00 from his employer backfired after a routine inspection unearthed the scam (Chadavaenzi 2014). A customer service training employee of FBC connived with a bank teller and swindled the Mines ministry over five hundred thousand dollars (Machakaire 2014). This shows that banks have been victimized by their employees who committed crime in their course of occupation.

1.2 Statement of the problem

As with other commercial banks and financial institutions internationally and regionally, Barclays Bank is in no way immune to the security challenges facing other banks. Barclays Bank, in its bid to make an appeal to the transacting public in terms of security in its operations has been in compliance with international banking standards like the BASEL committee. There have been cases of fraud in Zimbabwe, and no bank would want to leave loopholes in their security systems, thus the need to review security systems regularly. A significant number of breaches in the security systems are reported each year, drawing attention to the need to protect and inform customers about the risk of exposure to malicious actions initiated by fraudulent criminals. Financial institutions and consumers recognize the fact that fraud is becoming more complex and is perpetrated by a different classes of criminals. The classes are increasingly becoming sophisticated and use technology as part of their strategy.

If due respect in not given to fraud, banks will continue to suffer losses, bad publication will scare away investors and erode depositors confidence which may lead to bank failure. This has caused the need for the researcher to want to carry out this study which evaluates the impacts of white collar crime in commercial banks particularly Barclays Bank.

1.3 Objectives of the Study

- To establish factors contributing to fraud in the banking industry
- To highlight and examine the types of frauds committed against banks
- To determine appropriate strategies of preventing and controlling fraud

1.4 Research questions

- What are the types of fraud experienced at Barclays Bank?
- What are the impacts of fraud faced by Barclays Bank?
- What ways can be employed to combat fraud at Barclays Bank?

1.5 Assumptions

- There is effective bank security which reduces crime in the banking sector.
- Losses to fraud have a negative impact to the banking sector
- Fraud in commercial banks erodes bank's profits
- Information gathered from Barclays Bank is true and not biased

1.6 Significance of the study

Theoretically by investigating crime on business the researcher is going to add value on business intelligence and efficiency knowledge. It also seeks to offer a foundation for further research by other students pursuing similar research.

<u>To the researcher</u>

The researcher will have an in depth knowledge about the various impacts made by fraud on banks and other financial institutions.

To Bindura university

The research is going to be conducted in partial fulfillment of the Bachelor of Commerce Honor's Degree in Financial Intelligence. It is going to be of interest and hope of the researcher that the valuable information will provide hands on knowledge to students wishing to focus on the aspects of fraud thus evaluating their overall impacts on banks.

To Barclays bank Zimbabwe

- Using the research findings, conclusions and recommendations arrived at by the researcher, management and other users affected by fraud will gain knowledge and understand various impacts it has on banks and its stakeholders.
- The organization under study will be informed about its actual position with regards to fraud and be in a position to identify its strength and weaknesses pertaining to bank security hence benchmarking itself with its competitors.
- The organization will be able to forecast and predict the future behavior of its competitors based on research findings.

1.7 Delimitations of the study

The research on bank security and fraud prevention covering period (2010 to 2015) was conducted on Zimbabwe's banking sector using Barclays Bank Zimbabwe as case study.

1.8 Limitations of the study

- The researcher was facing financial constraints during the research process for example commuting, internet surfing and printing of questionnaires.
- The researcher was also having barrier to access of information because of confidentiality of information.
- The researcher also encountered bias caused by some respondents who viewed the research as a witch hunt.
- The researcher also faced lack of maximum participation by some respondents as they were too busy to attend to questions on the questionnaire

1.9 Justification of the study

The increase in number of reported cases of fraud involving large sums of money in actual and potential of late impact on profits and the competition in the banking industry has forced banks and other financial institutions to devise ways to improve security measures against white collar crimes particularly fraud and by so doing improve efficiency and profit output.

1.10 Definition of terms

Fraud: is a deliberate deceit planned and executed with intent to deprive another person of his property or rights directly or indirectly regardless of whether the perpetrator benefits from his or her actions. (Aderibigbe and Dada, 2007).

Efficiency: This is the comparison of what is actually produced or performed with what can be achieved with the same consumption of resources for example money, time and labor.

Business Intelligence: It is a process for extracting; transforming, managing and analyzing large data by makes a mathematical model to gain information and knowledge to help make decisions in the complex. It includes elements such as data warehouse, data mining and decision support system. (Jonathan, DMR 2000).

1.11 Summary

In this chapter, the researcher introduced the research study and gave the historical background of the problem to be solved. The significance of the study was discussed while the assumptions, limitations and delimitations were also discussed. The second chapter is going to be centered on relevant literature related to the evaluation of bank security to curb fraud. In essence chapter three is going to be centered on data gathering techniques and various tools will be used for collecting information needed for solutions to research questions.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

This chapter covers literature review, theoretical framework and empirical evidence relating to bank security and fraud preventing detection and investigation. Theories of security and crime prevention and investigation of fraud will be also to enlighten the reader on how fraud occurs. A detailed analysis of the Bank security and fraud will be carried out with primary sources of data and secondary sources such as textbooks and the internet will be used to give the research academic weight. This will help readers to have an overview of this topic.

2.1 Conceptual framework

Criminology theories

In criminology, examining why people commit crime is very important in the ongoing debate of how crime should be handled and prevented. Many theories have emerged over the years, and they continue to be explored, individually and in combination, as criminologists seek the best solutions in ultimately reducing types and levels of crime. Here is a broad overview of some key theories:

Rational choice theory

Becker, Gary (1968), postulates that the position of rational choice theory (RCT) is that criminal behaviour is no different from noncriminal behaviour in that it is conduct that persons intentionally choose to undertake (i.e., they are not compelled or forced to do crime), and the reason that they choose to commit crime is that they think it will be more rewarding and less costly for them than noncriminal behaviour.

Strain theory

Strain theories state that certain strains or stressors increase the likelihood of crime. These strains involve: the inability to achieve one's goals (e.g., monetary or status goals), the loss of

positive stimuli (e.g., the death of a friend, the loss of valued possessions) and or the presentation of negative stimuli (e.g., verbal and physical abuse).

Becker, Gary (1968), further states that individuals who experience these strains become upset, and they may turn to crime in an effort to cope. Crime may be a way to reduce or escape from strains. For example, individuals may steal the money they want or run away from the parents who abuse them. Crime may be used to seek revenge against the source of strain or related targets. For example, individuals may assault the peers who harass them. Crime also may be used to alleviate negative emotions; for example, individuals may engage in illicit drug use in an effort to make themselves feel better. Strain theories are among the dominant explanations of crime, and, as discussed in this research paper, certain strain theories have had a major impact on efforts to control crime.

Social disorganization theory

A person's physical and social environments are primarily responsible for the behavioural choices that person makes. In particular, a neighbourhood that has fraying social structures is more likely to have high crime rates. Such a neighbourhood may have poor schools, vacant and vandalized buildings, high unemployment, and a mix of commercial and residential property (Briggs, 2004)

Social Control Theory

Theorists believe it is society's responsibility to maintain a certain degree of stability and certainly in an individual's life, to make the rules and responsibilities clear, and to create other activities to thwart criminal activity. Drawing on the tenets of Routine Activity theory, Social Control theory is especially important when analysing crime in impoverished areas. The effect of poverty on the likelihood of crime is no secret nor is it a new phenomenon. When there is not enough food to eat or children are left alone at home while their parents work a second job, the seeds for crime have been planted and under this theory, it is society's obligation to prevent crime from happening. Various methods to provide children with social activities when their parents are unable to are very important in low-income neighbourhoods. Giving children an alternative to a life of crime is necessary under this theory of criminology (Tania, 2014).

Fraud defined

The Legal dictionary defines fraud as deliberately engaging in a secret scheme or deception intended to defraud a bank or financial institution, to obtain money or property owned by the bank or financial institution. Bank fraud is considered to be a white collar crime. A criminal charge of bank fraud generally applies when an individual knowingly executes, or attempts to execute, at act (1) in order to defraud a financial institution, or (2) to receive money, assets, credits, securities, or property from a bank or financial institution using false information, pretences, or insincere promises.

Woods, Ian (1998), states that Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. In many instances, bank fraud is a criminal offence. While the specific elements of particular banking fraud laws vary depending on jurisdictions, the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery or theft. For this reason, bank fraud is sometimes considered a white-collar crime

Fraud according to Adniji (2004) and ICAN (2006) is an intentional act by one or more individuals among management employees or third parties which results in a misrepresentation of financial statements. Fraud can also be seen as the intentional misrepresentation, concealment or omission of the truth for the purpose of deception or manipulation to the financial detriment of an individual or an organisation which also includes embezzlement, theft, or any attempt to steal or unlawfully obtain, misuse or harm the assets of the organisation, Adeduro, 1998 and Bostley and Drover, 1972. Fraud has increased considerably over the recent years and professionals believe this trend is likely to continue. Brink and Witt (1982), fraud is an ever present threat to the effective utilisation of resources and it will always be an important concern of management.

Weirich and Reinstein (2000), define fraud as “intentional deception, cheating and stealing”. Some common types of fraud include creating fictitious creditors, “ghosts” on the payroll, falsifying cash sales, undeclared stock, making unauthorized “write-offs”, and claiming excessive or never-incurred expenses. Pollick (2006) regards fraud as a “deliberate misrepresentation, which causes one to suffer damages, usually monetary losses” .Albrecht et al (1995) classified fraud into employee embezzlement, management fraud, investment scams, vendor fraud, customer fraud, and miscellaneous fraud. Fraud also involves

complicated financial transactions conducted by white collar criminals, business professionals with specialized knowledge and criminal intent (Pollick, 2006).

Fraud and banking

Traditionally banks have been defrauded, by fraudster depositing stolen cheques, forged altered cheques, fraudulent demand drafts, fraudulent procuring lines or credit by submitting fake documents (Deloitte, 2012). With increase in technology, methods of committing fraud have also increased in the banking industry. Banks are susceptible to white collar crime by virtue of collision of employees in their occupations.

2.2 Factors that Contribute to Fraud in Banks

Weak accounting systems

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 build-up of unbalanced posting, inadequate training, poor book keeping and genetic traits like kleptomaniac who pathologically steals for fund (Kingsley, 2012) .

Social factors

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 fewer than 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, these 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 in fact 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 perceive 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

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).

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 exist 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).

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).

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.

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 noncustomers of the banks and insiders /outsiders, which is a partnership of the employees (insiders) and outsiders.

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).

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).

Third Party Fraud

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

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 are 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).

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).

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. Akinyomi (2012) impersonation is particularly very successful where the outsider works in collaboration with an insider.

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. Onkagba (1993) counterfeit documents may be copied, forged or simply changed in its details e.g. dates, terms of payment or holder.

Money Transfer Fraud

Money transfer services refer 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).

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).

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).

Card Fraud

This is committed at ATMS and post terminals. 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 renter his or her security code. When the card holder leaves, the fraudster retrieves the card and renters 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 Causes of fraud

Sutherland, Edwin, (1947) coined the term white collar crime and was the driving force bringing it into the mainstream of criminology. Sutherland's original definition of white-collar crime was broad and encompassing, but in practice he focussed primarily on crimes committed by business and the corporations. Coleman, (1992) constructed an integrated theory that weaves all theoretical strands together into some kind of coherent whole. The approach that Coleman thought worked best was based on a simple common sense idea widely used in criminology. A crime will occur only if there is a confluence of an appropriate motivation and available opportunity.

Financial problems

Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware that this problem can be secretly

resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property. (Cressey, 2013)

Opportunity

By itself the non-shareable problem will not lead an employee to commit fraud (Wells, 2014). The employee must also perceive that he/she has the opportunity to commit the crime without being caught. While the position of trust may provide an opportunity for the solution of a non-shareable financial problem, Cressey (2013) found that many trusted people did not at first see in their positions of trust the opportunities which such positions offer, and thus did not engage in fraud by using entrusted funds to solve their non-shareable problems. Making the connection between the non-shareable problem and the illegal solution is a product of the interrelated intellectual processes of knowing and rationalizing that the problem can be solved by violation of their position of trust.

Rationalization

The act of rationalization is not an after-thought that justifies the fraud, but it is the real reason(s) which the person has for acting in a fraudulent manner. Rationalization is, therefore, part of the motivation to commit fraud and is often abandoned after the criminal act has taken place (Wells, 2014). Cressey (2013) observed that a trusted person does not invent a new rationalization for his violation of trust, but rather he applies to his own situation a verbalization which has been made available to him by virtue of his having come in contact with a culture in which such verbalizations are present. The fraudulent individual acquires such verbalizations from other persons who have had prior experience with situations involving positions of trust and trust violation.

Job dissatisfaction

Research by Hollinger and Clarke (2011) on 12,000 employees revealed that dissatisfaction motivated employees to commit fraud. When employees perceived that their jobs or working conditions were unfair, they were more likely to justify and commit fraud (Wells, 2014). However, this theory is difficult to prove due to the relative lack of information regarding employee theft in general; while it can be studied in its particulars, it is difficult to identify in

general due to lack of reliable and widespread information about employee theft (Mustaine & Tewksbury, 2012).

Capability of the offender

Wolfe and Hermanson (2013), argued the offender requires the capability of committing the crime, where capability may involve the technical knowledge, confidence etc. to execute and/or get away with the crime (Wolfe &Hermanson, 2013).

Criminal behaviour is learned

Sutherland (2009) suggested that criminal behaviour is learned. However, it differs from the Differential Association theory in that it presupposes the existence of a specific criminal culture, which is associated with people living in a specific area or within a specific ethnic group (Costello, 2012). He assumes that criminals have been transmitted into a culture of crime by being socialized to accept specific values that condone crime. Therefore implying that fraudulent behaviour in accounting is learned.

Misfit between values and norms

When there is a misfit between values and norms e.g. the dilemma between goals and the means to achieve it. In a bid to align the goals with the means an individual may adopt five types of solutions, including conformity, innovation (using illegitimate means to achieve success, as in accounting fraud), ritualism, retreats, and rebellion (Durkheim, 2014; Merton, 2012; Merton, 2011). All these adaptations arise from the pressures of the society that accentuate economic success and the difficulty of achieving it.

2.5 Impacts of Bank Fraud

The effects of fraud in the banking industry are felt by all, if not as a customer, then, as a citizen of nation. The effect of fraud has a chain reaction on the community as a whole because this industry constitutes a vital position in a community.

It destroys the bank's reputation

Despite the amount of money that banks put into risk management, be it operational, investment, or political risk, there is one area that banks have traditionally only mentioned in passing, that of reputational risk. Now that is not to say that banks haven't acknowledged

reputational risk. Indeed back in 2005, the Economist Intelligence Unit found that "52 per cent consider reputation risk as a risk by itself, while 48 per cent consider it as a consequence of other risks" like operational risk – people, process, systems and external events – compliance.

The trust and understanding among staff is reduced

Trust among co-workers, managers, and other bank team members is built, confirmed, weakened, or destroyed every day. Trust increases slowly over time through repeated interactions—but can dissolve in moments from just one bad criminal activity.

Fraud reduce bank's profitability.

Fraud leads to loss of money belonging either to the bank or customers. Such losses may be absorbed by the profits for the affected trading period and this, consequently, reduces the amount of profit which would have been available for distribution to shareholders. Losses from fraud, which are absorbed by the equity capital of the bank, impair the bank's financial health and constrain its ability to extend loans and advances for profitable operations. In extreme cases, rampant and large incidences of fraud could lead to a bank's failure.

It places emotional and psychological burdens on the fraud victims

There is a perception among some members of the public that fraud is a 'victimless' crime or has little impact (Duffield and Grabosky, 2011). The impact of fraud can also lead to a range of health problems, both physical and mental. Spalek (2012) in a study on the victims of the Maxwell pension fraud found that 'anger' was a common emotional impact of the fraud. She also found they suffered stress, anxiety and fear as a result of their loss.

It discourages banking habit among the banking public

Fraud as witnessed in recent times has resulted in the collapse of many banks, this raises the question of how reliable are banks to trust ones money with them, the ethics of banking profession which is honesty, reliability and competence are far fading away.

The bank ceases to meet up with staff welfare

The Bank is fully committed to supporting the health and welfare of its employees. These include insurance, paid leave (both annual and sick leave), social event activities such as team

building or parties. But with reduced profits through bank fraud the bank will not be able to meet the above staff welfare

2.6 Prevention and control of Bank Fraud

Types of fraud encountered in the banking environment include internal fraud and external fraud (Black, 2014b; Greenbaum & Thakor, 2010; Mishkin, 2011; Weiss, 2013). Fraud detection and prevention is at the heart of every fraud management system. Detection of fraud is highly complex, and a large percentage of fraud cases are actually detected externally (such as by the media or external auditors) or by accident (Dyck, Morse, & Zingales, 2010). However, approaches such as lifecycle monitoring and verification can be used to reduce the incidence of fraud overall (Potter, 2012; Porter, 2010; Wilhelm, 2013; Venkatraman & Delpachitra, 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).

Creating an Encouraging Work Atmosphere

Positive and good working environments enhance 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 behaviours include practices that deal swiftly with incidents and protect whistle blowers (ACFE, 2009).

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 behaviours 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).

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.

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, pre-emptive

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.

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).

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).

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).

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 analyse 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.

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).

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 defence, 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).

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 analyse 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

Auditing

Often a strong system of internal controls is the frontline defence that an organization can employ to prevent and detect fraud. The absence of internal controls does not always preclude the occurrence of fraud but it does leave potentially an open door for it to happen. Poor internal controls manifest themselves through: poor inventory control, lack of proper documentation and support for cash payments, lack of segregation of duties, ineffective or obsolete accounting software and the absence of independent verification (Doyle et al, 2014; Porter, 2013). To prevent these failures, companies should conduct periodic risk assessments, led by either internal or external auditing staff.

Whistle blowers and regulatory requirements

Whistle blowing is traditionally a voluntary practice of individuals who observe something incorrect about a given auditing or accounting situation and bring it to the attention of auditors (Schmidt, 2014). However, there has also been a movement in recent years to introduce a regulatory requirement for whistle blowers, or to induce some regulatory compensation or incentive to blow the whistle (Schmidt, 2014).

Supervision

Bank fraud commonly emerges as a response to inadequate supervisory conditions (Evanoff & Kaufmann, 2014). Supervision at the government level is arranged in different ways depending on the jurisdiction. The European Union has a central and single bank supervisory structure, like the one we have here in Zimbabwe, unlike the United States which has shared bank supervision structures.

Restriction of Business

Although banks may not detect initial fraud, they will have much stronger reactions following disclosed fraud by customers (Graham, Li, & Qiu, 2012). Specifically, companies that are forced to restate their earnings face higher spreads and interest rates and more demand for securing of loans than those that do not, as well as higher fees; those that have restated due to fraud are even further penalized. Thus, the bank can use contract terms to protect themselves from information asymmetries identified through these restatements (Graham, Li, & Qiu, 2012).

2.7 Empirical evidence

Rahman (2014) carried out a study on the effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. The study aimed to providing perception of bankers towards the effectiveness of fraud and detection techniques. Based on 146 questionnaires received among managers and officers of Islamic banks in Malaysia, the findings indicated that the protection software application as the most effective component of fraud prevention techniques. Bank reconciliation password protection and internal control review improvement represents as the most effective techniques when assessing independently. Individually bank reconciliation accounted for the highest mean which were perceived as the most acceptable strategy that have contributed to the fraud prevention and detection in the bank. This was

followed by password protection and internal control review and improvement firewall installation. Increased attention by senior management, cash reviews and inventory observation. Despite the best attempts by the top management to eliminate fraud, there is no substantial solution for fraud other than creating awareness among their employees on the components of deterrence, prevention, detection, mitigation. Analysis, policy, investigation and prosecution must be simultaneously implemented as delineated under the fraud management lifecycle theory in order to effectively prevent and detect fraud within banks.

A study carried out by Rasheed et al (2012) focused on fraud and its implications for bank performance in the Nigerian banking system since the sector controls over 60% of assets and liabilities of the whole Nigerian financial system. The periods from 2004 to 2009, were considered for analyses. Nigerian banks made the highest profit when compared with the previous years under review. The mean score and standard deviation of total amount involved in fraud and banks‟ profits. The calculated r-value is 0.968 which is greater than the critical r-value of 0.879 at 0.05 level of significance and 5 degree of freedom. The results showed that there is a significant relationship between total amount involved in fraud cases and bank's profit. The amount of fraud cases in the banks does affect the profit of the banks. No wonder then that the Central Bank of Nigeria (CBN) gave a directive in 2011, to all banks on the need to compulsorily revert to ten digit number to mitigate fraud in the industry. Many of the banks that were distressed in the past met their waterloo because of the adverse effect of fraud in their banks. The study showed that fraud has adverse effects on banks performance in Nigeria. Without doubt, the menace of fraud has been the major source of bank distress. Nigerian banks‟ profits are adversely affected by the number of fraud cases and amount of funds involved in the fraud to steal money.

Njanike et al (2009), carried out a study on the effectiveness of forensic auditing in detecting and preventing fraud. It looked into different types of bank fraud frauds that required attention by forensic auditors in Zimbabwean banks. Noting pronounced types of bank fraud were credit card fraud, identity fraud, credit card fraud, account fraud, computer fraud and fraudulent RTGs. The study was administered by the use of questionnaires and personal interviews and document review. Auditors from thirteen commercial banks, four building societies and four auditing firms were used. Results from the research showed that forensic auditing has a role to play in the overall protection of bank assets. Forensic investigators have a mandate to detect potential bank fraud and if occasioned, conduct investigations of cases at

hand and at least suggest effective ways of preventing occurrence of such frauds. Those that are difficult to detect and investigate include those which are computer related or which the computer is used as a conduit to commit fraud. In Zimbabwe at least types of fraud discovered to be challenges in the banking institutions. Amongst these five are dominant which include cheques fraud, identity fraud, credit card fraud, computer fraud and ATM fraud which account for nearly 90% of bank losses.

2.8 Justification of the study

The ever evolving nature of technology probed the researcher to undertake this study in light of other researches on aspects relating to the topic. The majority of the researches carried out on bank security aspect were carried out some years ago and do not shed light on the present moment events in bank security which is developing at a fast rate. Some of the security mechanisms being employed in developed countries might tend to be expensive to set up and maintain, thus, some organisations in developing countries might consider forgoing the mechanism and its security enhancement capacity.

2.9 Summary

Related literature under study was reviewed in this Chapter. Discussed were the fraud detection, fraud prevention, fraud risks assessment, perceived role internal auditing and findings of other researchers concerning fraud and internal auditors. The following chapter is focused on research methodology, research instruments, data collection procedures and ethical issues.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

This chapter outlines the research methods used in carrying out the research. It gives an outline of the research design, research subjects, sampling method, research instruments used, and data analysis and presentation. It also highlights the population, sources and types of data presentation and analysis procedures.

3.1 Research Design and Justification

According to Partington (2001), research design is a framework or plan of study that guides the collection and analysis of data. The main objective of the research design is to provide results which are judged to be credible and resemble reality and are taken to be true and reasonable. Research design can be exploratory, explanatory or descriptive. In this study, descriptive case study was used.

Descriptive research refers to the type of research question, design, and data analysis that will be applied to a given topic. Descriptive statistics tell what is, while inferential statistics try to determine cause and effect. Descriptive study is used when researchers want to apprehend the characteristics of certain phenomena underlying a particular problem. The evaluation of Bank security entails for better understanding of the security measures, effects of security breaches, tools and methods employed in detection and prevention of fraud.

Descriptive research design is both qualitative and quantitative as the research seeks to collect data that permits us to ascertain the characteristics of the phenomena being studied. This design was found to be more suitable for this study as it greatly helped in discovering the association of different variables and is easy to apply. This design is cheap and can greatly reduce the financial constraint without negatively affecting the effectiveness of the research.

3.2 Target Population

Population is defined by Levin (1994) as a collection of all the elements we are studying and about which we are trying to draw conclusion. Cooper and Schindler (2003) define population as the total collection of elements about which we wish to make some inference. A research population thus refers to the total set of units in which the investigation is interested. A population is accordingly an aggregation of elements from which the sample is actually drawn from. The chosen population will be made up of 80 Barclays Bank Zimbabwe staff members.

Sample

A sample is a representative part of a target population taken to show what the rest of the population is like. It is ideally synonymous with the entire population conveniently scaling down the study elements where it is impossible to study the whole population. Levin (1994) defines a sample as a collection of some, but not all of the elements of the population under study, used to describe the population. The sample for this research was drawn from Barclays Bank headquarters staff members. The researcher made use of the Employee listing to get a record of the people in the various departments. It is therefore from this population that the researcher chose a sample to get information from. The researcher then drew a sample including employees from different departments using the stratified random sampling technique.

Sampling technique

The researcher will employ the stratified random sampling technique. Stratified random sampling is a modification of random sampling in which you divide the population into two or more relevant and significant strata based one or a number of attributes. In effect your sampling frame is divided into a number of subsets. A random sample (simple) is then drawn from each of the strata, consequently, stratified sampling shares many of the advantages and disadvantages of simple random or systematic sampling.

Sample Size

The sample of the research is more inclined to the e-banking and risk management personnel as they are heavily involved in the e-banking transaction security aspect. Other important players in this system are considered equitably. The respondents have been chosen on the

basis of their strategic influence on the security measures of fraud. The sample consists of a total of 16 fraud operations personnel, 12 risk management personnel, 5 accounts personnel and 4 human resource management personnel. All in all, the sample consists of 37 respondents.

3.3 Data Sources

Cooper and Schindler (2003) defined data as the facts presented to the researcher from the study environment. Data is set into two forms namely primary and secondary data. Primary data refers to data structures of variables that have been specifically collected and assembled for the current research problem. In this case, it is the data specifically collected to evaluate Bank Security to curb fraud.

Secondary data is data at hand prior to the research. The data would not have been collected to serve answers to the research questions but information can be drawn from such sources.

Secondary data already exist at the time of the research and was not originally gathered to answer the problem at hand. The study used primary data.

3.4 Research instruments

The technique of data collection for primary data was questionnaires. Interviews were also conducted to get clarifications on certain areas whenever there was need.

Questionnaires

Structured questionnaires were utilised to collect data in this study. This technique consists of a series of questions, each providing a number of answers from which the respondents can choose. There were also questions that the respondents answered by giving their opinion, observation or suggestion pertaining to what happens in their own organisations. This meant that both structured and unstructured questions were useful in this research.

The questionnaire also included closed-ended questions which depended on the data sought by the study on each particular research question. The questionnaire included both closed-ended questions that only provided a simple choice of answer such as ‘yes’ or ‘no’ and open-ended questions, allowing the respondents to fully express their answer. According to Kinnear et al (1990), closed ended questions include possible answers and subjects allowing

respondents to make choices among them. Close-ended questions provide a number of alternative answers from which the respondent is instructed to choose (Scandura and Williams, 2000). Open-ended questions required respondents to answer in their own words. They will be used because they do not restrict the respondent thus widening the scope of response obtained.

Advantages of using questionnaires

- They are economic, cost-wise.
- The respondents perceive them as more anonymous.
- High response rate due to the follow-ups.
- Responses obtained, especially from close-ended questions are fairly easy to analyse.

Disadvantages of using questionnaires

- Some respondents were unwilling to provide some information which is industrially sensitive.
- Respondents were not be able deduce to exact meaning of some of the questions as intended by the researcher.
- Some respondents found it difficult to find time to answer the questionnaire due to tight schedules at work.

Measures taken to overcome the weaknesses the questionnaire:

Inform respondents as to why the information was being collected and how results were going to benefit them. Respondents were asked to respond honestly and told that if their response is negative this is just as useful as a positive opinion.

The questionnaire was to be made anonymous.

The questionnaire was short and precise so as to avoid confusion.

Interviews

To gather primary data, the researcher also conducted interviews. An interview is a conversation with the respondent to gather data whilst cross validating questionnaire results. Responses were recorded through taking of notes. The researcher used face-to-face interviews in data gathering.

Advantages of using interviews

- Easy correction of speech: Any misunderstanding and mistake could be rectified easily in an interview. Because the interviewer and interviewee physically present before the interview board.
- Development of relationship: Relation between the interviewer and the interviewee easily developed through the interview. It increased mutual understanding and co-operation between the parties.
- Selection of suitable candidate: Suitable candidates were selected through interview because the interviewer would know a lot about the candidate by this process.
- Collection of primary information: Interview helped to collect the fresh, new and primary information as needed.
- Sufficient information: Sufficient information was collected through the interview process. Because the interviewer asked any question to the interviewee.
- Time saving: Interview helped to save time to select the best suitable candidate. Within a very short time communication was accomplished through the interview.
- Less costly: It was less costly than other process of communication. It was very simple, prompt and low cost method of communication.
- Increasing knowledge: Any interview increases the knowledge of both the interviewer and the interviewee. They can interchange their views and ideas.

Disadvantages of using interviews

- There are some limitations of the interview process. It is not free from defects. The disadvantages of the interview are discussed below:
- Incomplete process: Suitable candidate could not be selected by interviews only. The written test could have been more important than the interview.
- No record: In the case of the interview some confusion arose in the future as, there was no evidence that had been discussed during interview.
- Lack of attention: Much attention is required for a good interview. But sometimes it was observed that both the interviewer and the interviewee were less attentive. That is why real information was difficult to be collected.
- Costly: Generally, interview method is expensive.

3.5 Data validity and reliability

Hancock and Algozzine (2006) defined validity as the degree to which the instrument measures the concept the researcher wants to measure. Mitigation against invalidity of data was taken care of by ensuring careful design of individual questions, refined after the pilot test.

According to Scndura and Williams (2000) reliability refers to the measuring instrument's ability to provide consistent results in repeated uses. Mitigation against unreliability of data was taken care of. The researcher will ensure that the questionnaire will be of reasonable lengths. The strongest indicator of a high reliability of this study is that the scales applied are frequently used scales of prominent researchers with a professional purpose.

Pilot Testing

The questionnaire was tested before being distributed to the rest of the respondents. In the pilot test, five questionnaires were handed out to respondents; the respondents were to be interviewed on the clarity of questions in the questionnaire as well as their ambiguity in order to refine the quality of the questionnaire. This exercise provided assurances of reliable responses since respondents were expected to understand the questions fully and respond correctly.

3.6 Data collection procedures

This takes into account various ways and steps to be taken in administering instruments and data collection from the subjects under study. This procedure involves three steps; firstly, seeking permission from the organisation's administration, secondly making appointments with respondents and lastly distribution and administration of instruments on the subjects of the sample. The researcher will distribute questionnaires to the respondents either by e-mail or hand delivery. A header on each copy of the questionnaires will have a clause to clarify the role of the research and assured the respondents to the confidentiality of their responses. To make appointments, calls and emails were used.

Validity and Reliability of Findings

Reliability and validity are conceptualised as trustworthiness, rigor and quality in qualitative researches. It is also through this association that the way to achieve validity and reliability of a research gets affected by the qualitative researchers' perspectives which are to eliminate

bias and increase the researcher's truthfulness of a proposition about some social phenomenon using triangulation. Methodological triangulation involves using more than one method to gather data, such as interviews, observations, questionnaires, and documents (Denzin, 1978).

3.7 Data Presentation and Analysis Procedures

Data analysis is the process of systematically applying statistical and/or logical technique to describe and illustrate, condense and recap and evaluate data. Initially the questionnaires will be checked for physical completeness. Qualitative data from the open-ended questions will be analysed through content analysis whereby the researcher will count the recurrence of certain facts to facilitate the drawing of conclusions. Pie charts, tables and bar graphs will be used, in the next chapter to present and analyse the data that has been collected by the researcher.

3.8 Conclusion

The exploratory research method was used in the research. The chapter outlined sampling issues, type of data obtained and the methods of data collection and analysis procedures. The researcher will now move to the next chapter of data presentation, analysis and discussion of the research findings.

CHAPTER IV

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

This chapter represents findings from the questionnaires and interviews used in the research. The findings are presented chronologically answering questions used by research instruments in covering aspects understudy. Following from the presentation of data, analysis and discussions provides meaning and support from other researches which were done prior to the present study.

4.1 Response Rate

Table 4. 1: Questionnaire responses for Barclays Bank Zimbabwe employees

Department	Number of distributed questionnaires	Number of responded questionnaires	Response rate
Operations	10	10	100%
Bank management	6	5	92%
Accounts	12	12	100%
Audit	9	8	92%
Average	37	35	95%

A total number of 37 questionnaires were distributed to respondents. Of the 37 questionnaires distributed 35 were returned and were fully completed, translating to a 95% response rate as shown in the table above. This means that the majority of the selected sample elements were able to complete and return the questionnaires successfully. The high response rate is a result of the follow ups through email and telephone calls that the researcher did to the subjects where the questionnaires had been left.

Table 4. 2: Interview Response Rate

Meetings Planned	Meetings held	%
12	10	83.33%

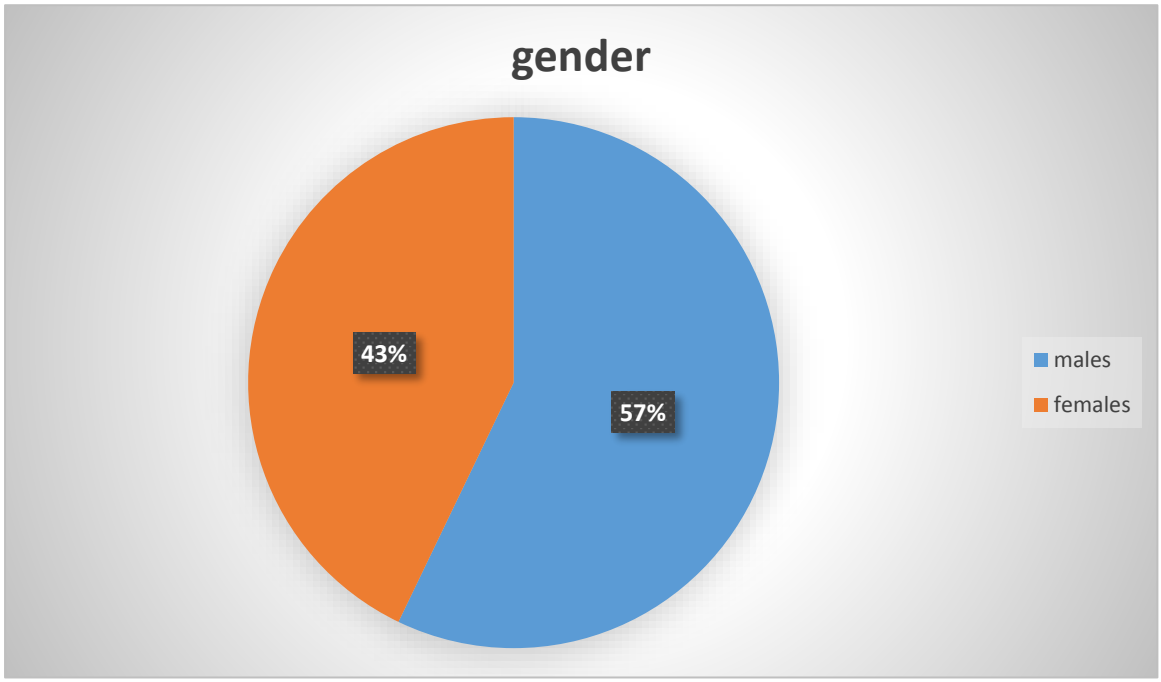
Source: Raw Data

Although the subjects had much work to do at their workplaces, most of them managed to give the researcher their attention relating to the personal interviews. From a target of twelve interviews, ten were successful and a failure of two resulted due to limited time and busy schedules for the people to be interviewed. Thus, ten meetings were held out of twelve without fail and pressure. This, resulted in 83.33 % response rate meaning that the results represented a true picture of the whole population since most meetings were held.

4.2 Demographic and industrial characteristics of the respondents

The study found the following distribution of respondents by gender;

Figure 4. 1: Gender of the respondents

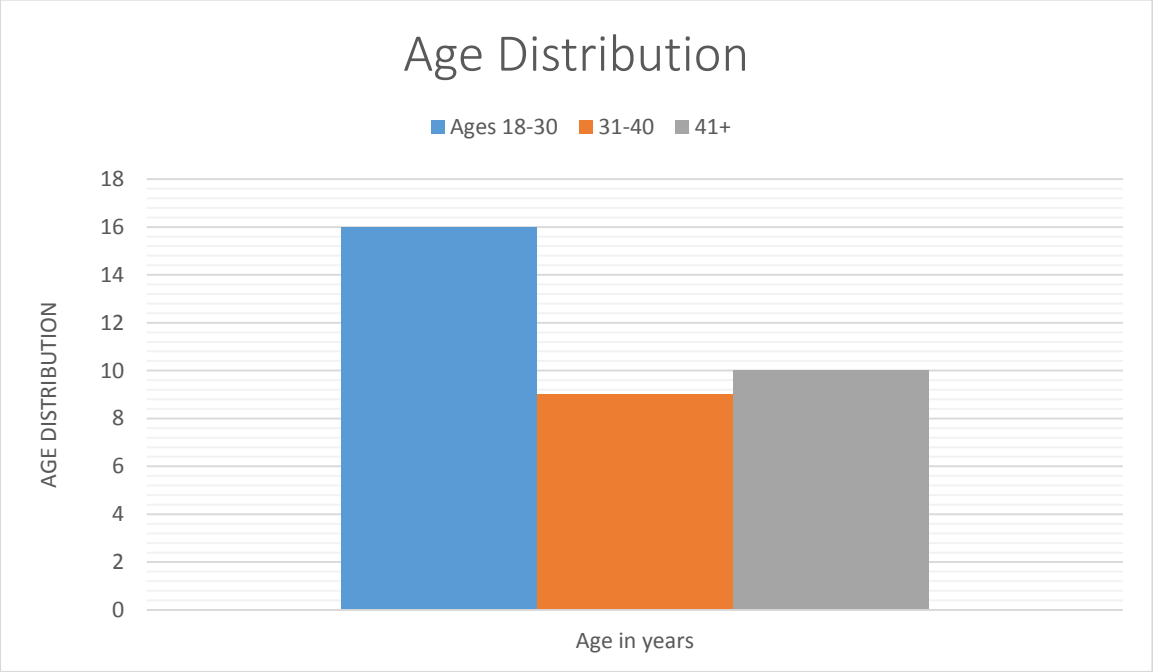


The distribution of the respondents by gender was 25(57%) were males and 15(43%) were females, this indicate that the sample selection procedure used ensured that the gender factor was well represented, hence the responses capture both gender as indicated in figure 4.1

Age of the respondents

The researcher sought to know the age distribution of the respondents, this is important in ensuring that the sampled respondents represents the age distribution of the entire population. This indicates that the sample was well distributed across various age group, therefore the response represents the views of employees with different experience on the subject matter. The age distribution of the respondent is presented in figure 4.2.

Figure 4. 2: Age distribution of the respondents



The age distribution of the respondents was; 16(45.7%) of the respondents aged 18-30 years, 9(25.7%) aged 31-40%, while 10(28.6%) aged 41-50 years.

4.3 Industrial characteristics

Respondents understudy possessed at least a professional course (25 %), first degree (35%), and a post graduate degree (40 %). These results show that the respondents in this study possessed the required information for the study either through qualifications or working experience and familiarity to the organisation. The response rate per subject was calculated as returned copies with respect to expected return of copies.

Table 4. 3: **Experience level**

Years of Experience	Frequency	Percentage frequency
0-5 years	5	14.28 %
6-10 years	8	22.85 %
11-15 years	13	37.14 %
Above 15 years	9	25.71 %

Source: Raw data

Results show that 5 (14.28 %), of the respondents have been working at Barclays Bank for years between 0 to 5 years, 8 (22.85 %) have been working for years between 6 to 10 years, whilst 13 (37.14 %) have been working for years ranging from 11 to 15 years and 9 (25.71 %) have been serving for more than 15 years.

These results show that the sample used represented the true and required population to acquire the desirable results.

Analysis of responses in relation to the meaning of fraud

The respondents were asked to explain what they understand by the term fraud, and all of them managed to define fraud in their own perceptions. They explained fraud as the misrepresentation of facts in order to gain a personal advantage. Others went on to explain that fraud is a financial crime committed by a person with a high social status. This entails that the subjects were aware of what fraud means. The researcher posed this question to the subjects in order to form a basis and an understanding from the subject's point of view in relation to fraud. The researcher felt that if the subjects understudy did not have an understanding of fraud, it was instinctive that they wouldn't know how fraud occurs.

4.4 Analysis of responses related to extent of fraud

Table 4. 4: Perceptions of the extent of fraud

QUESTIONNAIRES	Position of Respondents	
	YES	NO
Has there ever been a case of fraud in your organization?	74 %(26)	26%(9)
Is fraud a major concern in your organization?	63 %(22)	37%(13)

Source: Raw data

When respondents were asked if there were any cases of fraud that were witnessed at Barclays Bank, 74% of the respondents agreed to the notion that there were cases of fraud that were recorded at this institution. Table 4.4 goes on to show that 63% of the respondents agreed that fraud is a major concern at this institution and only 37 % disagreed that it is a major concern. The results show that there have been cases of fraud at this institution and this has proved that fraud is of major concern. The results of the extent of fraud are further presented in Figure 4.4 below:

The respondents were asked if there were any cases of fraud in their organisation and 80% of the respondents gave their perception that there were cases of fraud at Barclays Bank. Only 20% of the respondents did not agree with the fact that there were cases of fraud. This results shows that fraud is a major concern at this institution, evidenced by the cases of fraud that were recorded.

4.5 Analysis of responses related to the role and responsibility of auditors for fraud detection and prevention

Table 4. 5: Perceptions on the role of the internal auditor

Questionnaires	Audit	Management	Operations	Accounting Staff
Who is responsible for fraud detection?	35%	9 %	49 %	7 %
Who is responsible for fraud investigation?	0 %	0 %	100%	0%
Who is responsible for fraud prevention?	30 %	32 %	20 %	18 %

Table 4.5 shows that 35% of the respondents were of the opinion that the responsibility of fraud detection is in the hands of audit department, 9% were of the opinion that management is responsible for detecting fraud, 49% gave the opinion that the operations department is responsible for detecting fraud whereas 7% were on the opinion that the accounts department is the one responsible for detecting fraud. The same table also shows that all (100%) respondents were of the opinion that the operations department is responsible for fraud investigation. Respondents to questionnaires were also asked on whose responsibility it was on fraud prevention and 30% were of the opinion that the audit department is responsible for fraud prevention, 32% were of the opinion that the management is responsible for fraud prevention, 20% were of the opinion that the operations department is responsible for fraud prevention and only 18% were of the opinion that the accounting department is responsible for fraud prevention.

The results show that the subjects placed much responsibility on the operations department in fraud detection and investigation, however they held the management and audit departments responsible for fraud detection. Respondents pointed out some of the roles of the operations department pertaining to fraud detection, investigation and prevention. This included providing assurance of the effectiveness of internal controls, communication with the audit committee, management and legal advice about the allegations of fraud, helping to assemble

resources in different departments and work with the management, board of directors and other employees in preventing fraud and conducting proactive auditing to search out for fraud. In assessing the effectiveness of internal controls, the audit department participates in stock taking, verifies account balances, accuracy of double entry system, creation and maintenance of auditable fraud policy, fraud risk assessment or threat analysis, assistance in implementation, operation and maintenance of both internal and external fraud hotlines, and surprise fraud audits and also tests if accounting policies and practices are being followed.

Figure 3 further shows the respondents perception on the responsibility of fraud detection, investigation and prevention in relation to the internal auditor, management and accountants

4.6 Analysis of the responses related to the effectiveness of the internal controls in fraud detection, investigation and prevention.

Table 4. 6: Effectiveness of Internal Controls in detecting and preventing fraud

	Position of Respondents			
Questions	Very Effective	Effective	Moderately Effective	Not at all
Are internal controls an effective way of detecting and preventing fraud?	68%	20%	8%	4%

The results in Table 4.6 shows that 68 % of the respondents were of the opinion that internal controls are very effective in detecting and preventing fraud, 20% were of the opinion that internal controls are effective, 8% were of the opinion that internal controls are moderately effective and only 4% of the respondents were of the opinion that the internal controls are not at all an effective way of detecting and preventing fraud. Below is a pie chart which shows the respondents perception on the effectiveness of the internal controls in fraud detection and prevention.

4.7 Analysis of the responses related to the methods that are used to detect, investigate and prevent fraud.

The respondents were also asked the methods that they use in their organisation to detect fraud. In summary of the respondents' answers, complaints and whistle blowers indicates the activities of fraud. The respondents also highlighted the importance of checking excessive voids, missing documents, increasing reconciling items, and adjustments to receivables or payables and inventory shortages among other techniques. Respondents pointed out that fraud was best detected by bank security under the operations department, whistle blowers, and followed by incidents, audit, internal controls and notification by the police.

The respondents were also asked questions pertaining to the methods that are used to investigate fraud in their organisations. Almost 80% of the respondents emphasised on the importance of effective internal controls in fraud investigation. To summarise the methods given by the respondents, techniques used for fraud investigation fall into two primary classes. These are statistical techniques and artificial intelligence. An example of statistical data analysis technique is data processing techniques, validation, error correction and filling up of missing data. An example of artificial intelligence technique is pattern recognition to detect approximate classes, clusters or patterns of suspicious behaviour either automatically (unsupervised) or to match given inputs there is also machine learning techniques to automatically identify characteristics of fraud.

The respondents were also asked the methods that are used to prevent fraud in their organisations and 90% of them gave emphasis of the importance of the internal controls. The institution has established internal controls specifically designed to prevent and detect fraud and have also adopted a code of ethics for management and employees monitored by bank security under the operations department.

4.8 Discussion of the research findings

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

Factors Contributing to Fraud

Fraud is accorded high priority in Barclays Bank. The management of Barclays Bank 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 Barclays Bank lies with the fraud operations. Though very many causes of fraud exist in the Barclays Bank, the availability of opportunities for fraud was the most dominant factor. This study found that the most common cause of fraud in Barclays Bank 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 Zimbabwean banking institution.

The study sought to identify the specific factors that led to fraud in Barclays Bank. The specific factors with a high causative effect on fraud in Barclays Bank 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 build-up 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 Barclays Bank manages fraud in the organization. The study found that the Barclays Bank 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 Barclays Bank 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.

Types of Fraud

There are various types of frauds occurring in Barclays Bank. 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 Barclays Bank 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 Reserve Bank of Zimbabwe 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 Barclays Bank 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, and kitting. 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)

Prevention and Control of Fraud

There are various structures and systems embedded in Barclays Bank 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 centres 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.

4.9 Summary

The study focused on the presentation and analysis of data using methods outlined in the preceded chapter. The presentation was based of the findings obtained from the questionnaires and interviews. The next chapter gives summary findings, conclusions and recommendations to the study.

CHAPTER V

FINDINGS, CONCLUSIONS AND RECOMMENDATION

5.0 Introduction

This chapter is to focus on discussion of the results that were analysed in the prior chapter. After that, the researcher will give recommendations and provide some scopes for future research.

5.1 Summary of major findings

This study sought to assess the role of Bank Security to fight fraud in the banking industry in Zimbabwe using Barclays Bank of Zimbabwe 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 found that fraud in Barclays Bank 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 Barclays Bank 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 Bank Security had very effective strategies in place 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.

5.2 Conclusions

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

Factors Contributing to Fraud

This study concludes that the most dominant factor influencing or accelerating fraud in Barclays Bank 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.

Types of Fraud

This study concludes that employee fraud is the most common form of fraud in Barclays Bank. 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 Reserve Bank of Zimbabwe (RBZ) have been effective in containing management fraud. This is because management fraud in Barclays Bank was very rare.

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.

With all being said we can safely conclude that Bank Security has a major role in curbing fraud as it is responsible for monitoring, prevention and control of fraud evidenced by the research findings.

5.3 Recommendations

The following recommendations are made:

Recommendations for Practice

- These recommendations are for policy making at the organization and or industry level. Furthermore, these recommendations can be utilized at the practice or management level.
- 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 Bank Security should implement systems and structures that reduce the opportunities for fraud. In addition to strengthening internal control systems and structures, Security can use ICT tools to reduce opportunities or instil 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 RBZ 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.
- 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, claiming of unearned benefits and abuse of staff current accounts. 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 Security should instil 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 post-dated kitting, review or change of details in cards.

- 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 that Bank Security strengthen internal controls and accounting systems, the use of analytical tools to analyse and present statistics on fraud, use of audits and employee fraud schemes to combat fraud. Specifically, every bank must have fraud operations units where all fraud related incidences are investigated and reported.

5.4 Recommendations for Future Studies

The study recommends that future research be done on computer crime that affects banks since development of technology provides various ways of committing more sophisticated ways of committing fraud in banks.

REFERENCES

Adeniji, A. (2004): Auditing and Investigation. Lagos, Value Analysis Publishers.

Aderibigbe, P. and Dada, S. O. (2007): Microauditing Principles. Lagos ICAN Students Journal,Vol 11 No 1, Jan/March.

Adam, R. (2011). Preven'8t, protect, pursue - a paradigm for preventing fraud. Computer Fraud and Security, 7.

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

Bolton, R. J., & Hand, D. J. (2012). Statistical fraud prevention: A review. Statistical Science, 17.

Coenen, T., 2008. *Essentials of Corporate Fraud.* New Jersey: John Wiley & Sons.

Cressey, D. (1973). Other People's Money: A study in the social psychology of embezzlement. New Jersey: Patterson Smith Publishing Corporation

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

Chidavaenzi,P. 2014. Bank employee in court over fraud.Newsday January 21

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

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 Zimbabwe. Government of Zimbabwe.

Deloitte Touche Tohmatsu, 2010.The Inside Story, The Changing role of Internal Audit in dealing with financial fraud: Internal Audit Fraud Survey 2010, DTTL London

Elliot, R. K., & Willingham, J. J. (2010). Management fraud: Detection and deterrence. New York: Petrocelli Books.

Gaylord, M.S. and Galliher, J.F. (2012). The Criminology of Edwin Sutherland. New Brunswick, NJ: Transaction Books.

Gottschalk, P., 2010. *Policing Cyber Crime.* 1st Ed. New York: Peter Gottschalk & bookboon.com.

Gottschalk, P., 2010. *White-Collar Crime: Detection, Prevention and Strategy in Business Enterprises.* Florida: Universal Publishers.

Kaseke, K.2014. Steward Bank Employee up for $37K fraud. The Sunday times. May 25

Khanna, A., 2009. A study to investigate the reasons for bank frauds and the. Journal of Business Science and Applied Management, IV (3), pp. 1-21.

Mbaku, J. M. (2014). Corruption in Africa: Causes, consequences and clean-ups. London: Lexington Books.

Machakaire, T.2014. Banc ABC ex-employee up for $1m fraud. Daily News. June 12

Machakaire, T, 2014. FBC Bank tellers up for $500k fraud. Daily News. January 31

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

Njanike, K., Dube, T. & Mashayanye, E., 2009. The effectiveness of forensic auditing in detecting, investigating and preventing bank frauds. Sustainable development in Africa, Volume x, pp. 1-18.

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

Pollick, M.Y. (2006). What is Fraud: http://www.wisegeek.com/what-is-fraud.htm Accessed: 15 February 2010.

Porter, B. (1997): Auditors' responsibilities with respect to corporate fraud: a controversial issue, in Sherer, M. and Turley, S. (Eds), 3rd ed., Current Issues in Auditing, Paul Chapman Publishing. London, Ch. 2:31-54.

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.

Schutt, R. K. (2013). Investigating the social world: The process and practice of research. Newbury Park, CA: Pine Forge Press.

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

Weiss, J. W. (2009). Business ethics: A stakeholder and issues management approach. 5th ed. Cincinatti, Ohio: Cengage Learning.

Wells, J. (2014). Corporate fraud handbook: Prevention and detection (2nd ed.). London: John Wiley and Sons.

Williams, H. E., 1997. Investigating White Collar Crime: Embezzlement and Financial Fraud. 2nd ed. Springlefield: Charles C Thomas Publisher Ltd.

Wilson, 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.

LIST OF APPENDIXES

APPENDIX 1

QUESTIONNAIRE COVER PAGE

BINDURA UNIVERSITY OF SCIENCE EDUCATION

REF: Request for completion of a Questionnaire

I am a student at Bindura University studying for a Bachelor of Commerce (Honours) Degree in Financial Intelligence and undertaking a research project **on the evaluation of bank security and fraud prevention (case study of Barclays Bank Zimbabwe).**

This research seeks to establish different types and impacts of fraud and suggest ways of combating fraud at Barclays Bank using questionnaires and interviews to obtain both qualitative and quantitative data.

In going about the research, I shall respect criminological research ethics that is respect at all times the confidentiality of the respondents with all data sampled treated in the utmost confidence and the completed questionnaires processed only by me.

I kindly therefore request you to assist by completing the attached questionnaire giving honest answers to questions to the best of your knowledge. The questionnaire is designed purely for academic purposes only and the information provided shall thus be treated as highly confidential.

Participation in this study will be voluntary. The data collected will be kept securely for 5 years for purposes of verification.

Your co-operation is greatly sought

Yours faithfully

Taurai V Chigova

APPENDIX 2

QUESTIONNAIRE

(PRIVATE AND CONFIDENTIAL)

INSTRUCTIONS:

- Indicate by way of a tick (√) the relevant answers and provide information in the spaces provided were necessary.
- Please do not write your name on the questionnaire.

Section A

1. Name of organisation……

2. Years of experience in the organisation

0-5 years ☐ 6-10 years ☐

11-15 years ☐ above 15 years ☐

3. Current position.....

4. Qualifications.....

Section B

1. What do you understand about fraud?

.....

.....

.....

2. Has there ever been a case of fraud in your organisation?

Yes ☐ No ☐

a. If the answer is yes, how did it happen?

.....
.....
.....

b. If there are cases of fraud in your organisation, can you give the types of fraud that you witnessed?

.....
.....
.....
.....

c. Is fraud of major concern in your organisation?

Yes ☐ No ☐

3. What are the responsibilities of Bank Security in your organisation?

.....
.....
.....
.....
.....

4. In your opinion whose responsibility is it to detect and prevent fraud in Barclays Bank?

Audit ☐ Management ☐

Accounts ☐ Operations ☐

All employees ☐

Give an explanation for your answer?

.....
.....

5. Whose responsibility is it to report fraud in Barclays Bank?

Audit ☐ Management ☐

Accounts ☐ Operations ☐

All employees ☐

Give reasons for your answer?

.....

.....

6. Whose responsibility is it to investigate fraud in the Bank?

Audit ☐ Management ☐

Accounts ☐ Operations ☐

All employees ☐

Give reasons for your answer?

.....

.....

7. In your opinion what are internal controls In Barclays Bank?

.....

.....

.....

a. Are internal controls an effective way of detecting and preventing fraud in the Bank?

Effective ☐ Very effective ☐

Moderately effective ☐ Not at all ☐

Give reasons for your response

.....

.....

.....

.....

8. What are the processes and methods used to detect fraud in your organisation?

.....

.....

.....

.....

.....

.....

9. What are the methods that are used in investigation fraud in your organisation?

.....

.....

.....

.....

.....

.....

10. What methods does your organisation use in preventing fraud?

.....

.....

.....

.....

.....

.....

.....

11. What is your opinion on the role of Bank Security in relation to fraud prevention, detection and investigation to your organisation?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Thank you for your assistance

APPENDIX 3

INTERVIEW GUIDE

I would like you to assist me with some answers and comments to the following questions on **the evaluation of Bank Security in fraud detection, investigation and prevention.**

1. In your own understanding, what do you understand by the term fraud?
2. Are there any recorded cases of fraud in your organisation?
3. Who then is responsible for the detection of fraud?
4. After fraud has been detected, the suspects need to be investigated and those found guilty penalised. Who is responsible for this investigation?
5. If fraud is prevalent it needs to be prevented to avoid future losses, who is supposed to prevent it?
6. What are the methods that can be used to prevent fraud?
7. What is the role of Security in your company?

Thank you for your assistance