COMMERCIAL BANKS RESPONSE STRATEGIES TO FRAUD-RELATED CHALLENGES

BY

RAPHAEL WANGA

UNITED STATES INTERNATIONAL UNIVERSITY

SPRING 2013
COMMERCIAL BANKS RESPONSE STRATEGIES TO FRAUD-RELATED CHALLENGES

BY

RAPHAEL WANGA

A Project Report Submitted to the Chandaria School of Business in Partial Fulfillment of the Requirement for the Degree of Global Executive Masters in Business Administration (GeMBA)

UNITED STATES INTERNATIONAL UNIVERSITY

SPRING 2013
STUDENT’S DECLARATION

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

Signed: _______________________  Date: ___________________

Raphael Wanga (ID: 636233)

This project has been presented for examination with my approval as the appointed supervisor.

Signed: _______________________  Date: ___________________

Prof. Francis W. Wambalaba
Supervisor

Signed: _______________________  Date: ___________________

Dr. George Achoki
GEMBA Coordinator

Signed: _______________________  Date: ___________________

Dr. George Achoki
Dean, School of Business
ABSTRACT

The general objective of this study was to determine the responses by Commercial banks to fraud related risks in the banking industry. Specifically, the study sought to establish the effect of fraud detection strategies on fraud related risks in the banking industry, to determine the effect of fraud prevention and control strategies on fraud related risks in the banking industry and to establish how responses by commercial banks in Kenya to fraud related risks in the industry can be improved.

This was a case study since the unit of analysis was one organisation aimed at getting detailed information regarding the strategic responses to increasing fraud risk at commercial banks. Primary data was collected using self-administered questioners. The questioners contained closed and open-ended questions. The open-ended questions enabled the researcher to collect qualitative data. Before processing the responses, the completed interview guides were edited for completeness and consistency. A quantitative analysis was employed. The quantitative analysis was used to analyze the questioners about the strategic responses to fraud risk in commercial banks.

The study found that there are fraud detection strategies adopted by commercial banks in Kenya. There was no single test that a fraud has been committed. The study found that there are fraud prevention strategies adopted by commercial banks. The banks adopt fraud prevention strategies to some extent. There is a Group Fraud Policy that’s applicable to all Commercial banks in the world. The bank also carries out a random check christened “the Eye-ball”. This is a random selection of account opening documents by a dedicated team of Fraud Samplers. The study also revealed that a whistle blowing facility is existent in the Bank. The study found that the bank has a fraud control plan documenting the responsibilities for fraud prevention, detection and response initiatives.
The study concludes that fraud is very sensitive and that customers have immense fear of fraud and it impacts negatively on banks profitability where income lost through fraud would have been reinvested to foster growth. Higher profits for a business will indicate that a Bank management is having the right strategy thus sending a positive signal to the market. The study also concludes that the worst fraud risk is identity theft where identification documents are easy to reproduce, fraudsters make parallel passports, IDs and driving licenses then use them to take over accounts. The study further concludes that cheque fraud is a common type of fraud mainly because customers with cheque books are not careful in ensuring that their books are kept in safe custody.

The study recommends that there should be reforms in the police. This could help reduce the fraud related risks in the bank. The study recommends that since the judiciary is a key player in Fraud Management and that over the time, it has been seen that courts often acquit or hand in lenient sentences to deadly fraudsters, the judiciary needs to be empowered through reform to be able to understand and be of help. The study also recommends that review of Fraud Legislation could reduce fraud related risks in the banks. Kenya still lags behind on anti fraud laws. The study also recommends that review of security features of security documents (The Kenyan National ID, Driving licenses, passports and Title deeds) would also eliminate fraud related risks in the bank. Other recommendations suggested include staff management where human beings need constant monitoring and motivation of staffs. Appropriate methods should be put in place deal with the situations. Methods such as employee screening, staff account monitoring, profiling of staff disciplinary cases, job rotation and enrichment are worth considering.
DEDICATION
ACKNOWLEDGEMENT
# TABLE OF CONTENTS

STUDENT’S DECLARATION ........................................................................................................ iii
ABSTRACT .................................................................................................................................. v
DEDICATION .............................................................................................................................. vii
ACKNOWLEDGEMENT ............................................................................................................... viii
TABLE OF CONTENTS ............................................................................................................... ix
LIST OF TABLES ....................................................................................................................... xi
LIST OF FIGURES .................................................................................................................... xii
LIST OF ABBREVIATIONS/ACCRONYMS ............................................................................... xiii
CHAPTER ONE ........................................................................................................................ 1
  1.0 INTRODUCTION ............................................................................................................... 1
    1.1 Background of the Study ................................................................................................. 1
    1.2 Statement of the Problem ............................................................................................... 6
    1.3 General Objective ........................................................................................................... 7
    1.4 Specific Objectives ......................................................................................................... 7
    1.5 Significance of the Study ............................................................................................... 7
    1.6 Scope of the study ........................................................................................................... 8
    1.7 Definition of Terms ......................................................................................................... 9
    1.8 Chapter Summary ......................................................................................................... 9
CHAPTER TWO .......................................................................................................................... 11
  2.0 LITERATURE REVIEW .................................................................................................... 11
    2.1 Introduction ..................................................................................................................... 11
    2.2 Fraud Detection Strategies ........................................................................................... 11
    2.3 Fraud Prevention Strategies ......................................................................................... 18
    2.4 Fraud Related Risks Responses Improvement Strategies ........................................... 27
    2.5 Chapter Summary ......................................................................................................... 30
CHAPTER THREE ..................................................................................................................... 31
  3.0 RESEARCH METHODOLOGY ......................................................................................... 31
LIST OF TABLES

Table 3.1: Target Population ............................................................................................................................. 32
Table 3.2: Sample Size ......................................................................................................................................... 34
Table 4.1: Response Rate ...................................................................................................................................... 38
Table 4.2: Whether there are fraud detection strategies adopted by Commercial Banks in Kenya .................................................................................................................................................................................. 42
Table 4.3: Extent that fraud detection strategies are adopted at the Commercial banks .............................. 42
Table 4.4: Extent that the respondents employ various fraud detection strategies in commercial banks ................................................................................................................................................................................................. 44
Table 4.5: Whether there was fraud prevention strategies adopted by commercial banks ....................... 45
Table 4.6: Extent that the aspects of fraud prevention strategies were adopted by the bank ........................ 47
Table 4.7: Respondents’ agreement level with statements that relate to fraud risks responses improvement strategies .................................................................................................................................................................................................................. 53
Table 4.8: Extent respondents agree that the banks should adopt the strategies to ensure optimal response to the fraud risk .................................................................................................................................................................................................................... 54
LIST OF FIGURES

Figure 4.1: Gender of the respondents .......................................................... 39
Figure 4.2: Respondents age bracket .............................................................. 40
Figure 4.3: Duration served in the Commercial banks ..................................... 40
Figure 4.4: Highest level of education ............................................................. 41
Figure 4.5: Extent that fraud prevention strategies adopted by the bank ........... 46
## LIST OF ABBREVIATIONS/ACCRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACEF</td>
<td>Association of Certified Fraud Examiners</td>
</tr>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>BCCI</td>
<td>Bank of Credit and Commerce International</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CPA</td>
<td>Certified Public Accountants</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resource</td>
</tr>
<tr>
<td>IFA</td>
<td>International Federation of Accountants</td>
</tr>
<tr>
<td>SAS</td>
<td>Statement on Auditing Standards</td>
</tr>
</tbody>
</table>
CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Study

Pearce and Robinson (2005) defined strategic responses as the set of decisions and actions that result in the formalization and implementation of plans designed to achieve a firm’s objectives. Banks respond to challenges in their operating environment in different ways. Ansoff and McDonnell (1990) noted that strategic responses involve changes in the firm’s strategic behaviours to assure success in transforming future environment.

The environment in which organizations operate is constantly changing with different factors influencing the organizations. Coping with the increasingly competitive environment has called on firms to rethink their marketing strategies (Pearce and Robinson, 2005). The days when firms could simply wait for clients to beat a path to their door are long gone. Organizations must realize that their services and products, regardless of how good they are, simply do not sell themselves (Kotler, 2000).

Critical information about risks residing within individual business units can be difficult to unearth without backing from senior management or the audit committee. Employees or middle managers, who often know where the skeletons lie, may be hesitant to furnish information because they fear suspicion, want to avoid the corporate spotlight, or harbor information about someone's misconduct perhaps even their own. Internal auditing can be hard-pressed to overcome this hesitancy unless the board or management actively supports investigation efforts.

Crime in Kenyan banks has evolved from simple crimes of petty theft and forgeries to hi-tech computer based cyber crimes. Fraud has manifested itself in various ways for example; Forgery which is an act of commission by an individual that result in falsification of document with intent
to cause deception or purported fraud. It is an act of making a copy or an imitation of something in order to deceive people.

Frauds in Kenyan banks only prove that financial liberalization aggravates the inherent tendency of shallow markets to foster excessive speculation and worsens the systematic consequence of such speculative activity. Revelations of fraud, evidence of insider trading and consequent collapse of investor interest have led to an almost unstoppable downturn in Kenyan banks. Bank frauds concern all citizens. It has become a big business today for fraudsters.

Failure to prevent and detect fraud has serious consequences for organizations. Although rare in occurrence, financial statement fraud can result in devastating losses to investors, creditors and auditors. Detecting fraud is a difficult task for auditors, in part because most have never experienced fraud in their careers (Montgomery et al., 2002; Pany and Whittington, 2001).

The Companies Act, the Banking Act, the Central Bank of Kenya Act and the various prudential guidelines issued by the Central Bank of Kenya (CBK), governs the Banking industry in Kenya. The banking sector was liberalized in 1995 and exchange controls lifted. The CBK, which falls under the Minister for Finance’s docket, is responsible for formulating and implementing monetary policy and fostering the liquidity, solvency and proper functioning of the financial system. The CBK publishes information on Kenya’s commercial banks and non-banking financial institutions, interest rates and other publications and guidelines. The banks have come together under the Kenya Bankers Association (KBA), which serves as a lobby for the banks’ interests and addresses issues affecting its members (Kenya Bankers Association, 2008).

There are forty-three commercial banks and non-bank financial institutions, fifteen micro finance institutions and forty-eight foreign exchange bureaus in Kenya. Thirty-five of the banks, most of which are small to medium sized, are locally owned (Central Bank of Kenya 2007). The industry is dominated by a few large banks most of which are foreign-owned, though some are partially locally owned. Nine of the major banks are listed on the Nairobi Stock Exchange. The banks have come together under the Kenya Bankers Association (KBA), which serves as a lobby for the banks’ interests and addresses issues affecting member institutions. The commercial banks
and non-banking financial institutions offer corporate and retail banking services but a small number, mainly comprising the larger banks, offer other services including investment banking, insurance services and custodial services among others (Dikken and Hoeksema, 2001).

Banks represent a significant and influential sector of business worldwide that plays a crucial role in the global economy. Commercial banks are financial intermediaries that serve as financial resource mobilization points in the global economy. They channel funds needed by business and household sectors from surplus spending to deficit spending units in the economy. A well developed efficient banking sector is an important prerequisite for saving and investment decisions needed for rapid economic growth. A well functioning banking sector provides a system by which a country’s most profitable and efficient projects are systematically and continuously funded. The role of banks in an economy is paramount because they execute monetary policy and provide means for facilitating payment for goods and services in the domestic and international trade (Shambe, 2003).

Commercial banks are custodians of depositor’s funds and operate by receiving cash deposits from the general public and loaning them out to the needy at statutorily allowed interest rates. Loans are based on the credit policy of the bank that is tightly coupled with the central bank interest rate policy. These in effect determine the level of financial risk in a particular bank.

Fraud is defined by the Malaysian Approved Standards on Auditing (2001), AI No. 240, as an intentional act by one or more individuals among management, employees, or third parties, which results in a misrepresentation of financial statements. Concise English dictionary defines fraud as an act of deceit, scam, con, cheat, hoax, scandal by means of false representation to obtain an unjust advantage.

Fraud is believed to be amongst the most serious corporate problems, and challenges in today's business environment, indeed Palshikar (2002) suggests that fraud or scam is a dominant white collar crime in today's business environment, many businesses and government organisations, particularly in financial and related services, suffer from fraud of various kinds. In the banking industry, many frauds are perpetrated through falsified payment instruments. Common fraud
types include; Cheque fraud, computer fraud, Card fraud and Mail order fraud that’s commonly referred to as internet fraud.

The phenomenon is empirically supported by a number of studies; for example, Cain (2009) and the KPMG Australia fraud survey (KPMG, 2002) each indicate that over 50 per cent of all interviewees surveyed believed that fraud is a major business problem. Similarly, reviews of fraud cases by Rezaee (2004) revealed that financial statement fraud has cost market participants more than $500 billion during recent years, with serious litigation consequences for associated auditors.

Fraud can be perpetrated on organisation both from outside – the external threat – and from within. Organisations can be set up for the principal purpose of defrauding others and, using the agency of a limited company; fraudsters can perpetrate serious economic offences shielding themselves behind the veil of incorporation. Fraud is now the crime of choice of organised criminal gangs worldwide. The likely gains are enormous and the likelihood of apprehension and thus of conviction and punishment comparatively small compared with conventional crimes of dishonesty involving guns, intimidation and violence of all kinds. Professional criminals are targeting big business.

The risks of fraud within and upon corporations cannot be understated. They include the immediate risks to the company affected, which can fail completely. There is also the reputation risk to the company that has suffered major fraud. This is one reason that companies and particularly financial houses are so reluctant to report fraud to law enforcement, where they fear that the likelihood of their names hitting the headlines associated with major losses will result in competitors’ obtaining an advantage and customers walking away. Systemic risk, that affects an entire financial market or system, and not just specific participants, cannot be underestimated. After the secondary banking crisis in the 1980s, where so many minor financial houses failed, largely as a result of fraud, confidence in the banking sector was shaken severely.

A possible strategy for auditors in light of this problem is to assess the likelihood of fraud. The ability of an auditor to accurately assess the risk of fraud is crucial to the initial assessment of
risk of material misstatement during the planning stage of the audit. The risk assessment will affect the design of audit tests. Incorrect assessment of risk may result in either inefficient or ineffective audit.

The value of internal control is apparent in both preventing and detecting fraud as prevention is better than cure. A weak internal control creates opportunities for fraud and about half of all frauds occur in the financial area (Valentine et al, 2002). Internal control system has four broad objectives; those are to safeguard assets of the firm; to ensure the accuracy and reliability of accounting records and information; to promote efficiency in the firm’s operation; and to measure compliance with management's prescribed policies and procedures. The effectiveness of internal control depends largely on management integrity.

Kazmi (2002) argued that maintaining security is a never-ending struggle. Just when one has an airtight system in place, a new hacker technology or an especially diabolical adversary enters the picture. The introduction and enforcement of controls will reduce the opportunities for fraud. The control warns potential fraudsters that management is actively monitoring the business and that in turn deters fraud (Clark, 2000). As a result, an organization, which seeks to contain computer fraud, should strive to implement a broad range of interventions, be it technical, formal or informal. Technical interventions are controls implemented to limit access to building, rooms or computer systems. Formal interventions involve horizontal expansion of the hierarchy of organization to have a flatter pyramid. Education, training and awareness programmes are some measures implemented in the informal interventions. Controls have dysfunctional effects because isolated solutions have been provided for specific problems. These “solutions” tend to ignore other existing controls and their contexts. Thus, individual controls in each of the three categories, though being important, must complement each other. This necessitates an overarching policy, which determines the nature of controls being implemented, and therefore provides a comprehensive security to the organization.
1.2 Statement of the Problem

The fraud scandals involving corporations like Enron, Adelphia, Global Crossing, Parmalat, Tyco and Xerox have resulted in financial statements credibility loss raising questions about the Accounting and Auditing profession. Consequently, some countries created various oversight regulatory bodies to interrogate the financial reporting aspects. Countries like the USA developed certain laws to place more accountability on companies and top executives (Sarbanes-Oxleyact, 2002). Former SECs president Lynn Turner (2009) states that “given the fact that accounting is done by people, I do not expect us to be able to totally eliminate fraud. However, we should not ignore it but rather proceed with timely and appropriate enforcement actions”.


A large body of research has focused on the fraud risk assessment process. For example, these studies have examined the effects of making separate risk assessments for fraud, (Malaysian Approved Standards on Auditing), decomposing the risk assessment (Montgomery et al, 2002), and using decision aids such as a red-flag questionnaire (KPMG, 2002; Cain, 2009), or an expert system (Rezaee, 2004). Another group of studies has examined whether auditors adjust the nature and/or extent of planned audit tests based on their planning-stage fraud risk assessments (Valentine et al, 2002; Pany and Whittington, 2001).

Prior studies have found that failing to detect fraudulent financial reporting can expose the auditor to adverse legal and/or regulatory consequences. For example, Carcello and Palmrose (1994) and Palmrose (1987) found a significant positive association between the presence of fraud and litigation against the auditor.
The reviewed studies have focused on different aspects of fraud like detection and extent of its effects on different sectors of the economy. Further, most of them are on international scenes or on developed countries. To the researcher's knowledge, at the time of the study, no local or international studies had ever focused on the strategic responses adopted by banks in Kenya to counter increasing fraud risks. This was despite the ever increasing cases of fraud risks that had claimed a number of financial institutions in Kenya and thus calling for strategic responses to curb the spread of the crime. It was in this light that the researcher aimed to fill the existing gap by carrying out an investigation into the strategic responses to increasing fraud risks in the banking industry.

1.3 General Objective

The general objective of this study was to determine the responses by commercial banks in Kenya to fraud related risks in the industry.

1.4 Specific Objectives

1.4.1 To establish the effect of fraud detection strategies on fraud related risks in the banking industry.

1.4.2 To determine the effect of fraud prevention and control strategies on fraud related risks in the banking industry.

1.4.3 To establish how responses by commercial banks in Kenya to fraud related risks in the industry can be improved.

1.5 Significance of the Study

1.5.1 Commercial Banks

The study will be important to managers in the banking sector and to larger extent managers of other industries. It would help them understand the strategic responses and how its understanding can help different firms reduce or curb fraud related risks in their organizations and achieve
competitive edge. The study would also help other managers know the methods used in gathering and applying various strategic responses, which would help them improve their management styles.

1.5.2 Central Bank of Kenya

The study will also be invaluable to the Central Bank of Kenya as it will furnish it with information that they may use when coming up with guidelines and regulation governing the commercial banks to ensure fraud reduction.

1.5.3 Bank Customers

By establishing the responses by commercial banks in Kenya to fraud related risks in the industry, the study will inform the customers on the role they need to play on their part in curbing the menace. The customers will also gain confidence and trust with the banks after being informed of the responses they are adopting.

1.5.4 Researchers and Academicians

The study would also highlight other important relationships that require further research; this will be in the areas of relationships between fraud related risks and the strategic responses to impact on their performance. The results of this study would also be invaluable to researchers and scholars, as it would form a basis for further research. The students and academics would use this study as a basis for discussions on fraud risks and the strategic responses. The study will be a source of reference material for future researchers on other related topics; it would also help other academicians who undertake the same topic in their studies.

1.6 Scope of the study

The study investigated the commercial banks response strategies to fraud-related challenges. The management staff of all the commercial banks headquarters in Kenya provided the information needed. The researcher believed that these would provide an adequate population and sample for the study and therefore gave reliable results and findings.
1.7 Definition of Terms

1.7.1 Strategic Responses –

This is the set of decisions and actions that result in the formalization and implementation of plans designed to achieve a firm’s objectives.

1.7.2 Fraud -

This is an intentional act by one or more individuals among management, employees, or third parties, which results in a misrepresentation of financial statements. It is an act of deceit, scam, con, cheat, hoax, scandal by means of false representation to obtain an unjust advantage.

1.7.3 Fraudulent financial reporting (management fraud) – This is where management seeks to inflate reported profits or other assets by overstating assets and revenues or understate expenses and liabilities in order to embellish the financial statements.

1.7.4 Misappropriation of assets (employee fraud) is - where employees steal money or other property from their employers.

1.7.5 Accounting fraud - This involves an intentional action, leading to a misstatement in the financial statements.

1.7.6 Fraud detection - This entail of performing extended procedures necessary to determine whether fraud, as suggested by the indicators, has occurred. It includes gathering sufficient evidential matter about the specific details of a discovered fraud.

1.8 Chapter Summary

Chapter one presents the background information to the problem, identifies the problem statement, states the purpose of the study and lists the research questions that the research project will investigate. It also presents the rationale, scope and definition of the study to research on.
Chapter two presents the literature review. It discusses the existing research in the subject matter. The discussion tackles all the research questions posed and provides a firm theoretical background for the study.

Chapter three presents the research methodology proposed for this study. It details the research design, data collection methods, and how results will be analyzed. It covers the research design and justification, the target population, sampling and sample, data collection, and data analysis.

Chapter four presents analysis and findings of the study as set out in the research methodology. The results are presented on the responses by commercial banks in Kenya to fraud related risks in the industry. The study closes with chapter five which presents the discussion, conclusion, and recommendations for action and further research.
CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter discusses the past study on fraud risks in organizations. The specific areas covered here are concept of fraud, reasons for committing fraud and strategic responses to fraud risks.

2.2 Fraud Detection Strategies

Fraud detection can be categorized into technology-base and non-technology-based methods. Senator (2000) further categorizes technology-related methods into the following two categories: (1) Computerized traditional methods and (2) strategic methods. Strategic methods can be subdivided into those that (2a) focus on people and (2b) focus on transactions and reports. Focusing on people includes methods such as using artificial intelligence techniques and fuzzy logic to score personnel profiles or matching individuals against known ‘bad guy’ lists. Focusing on transactions involves searching records and databases for fraud symptoms relating to sales, purchasing, payment, receipt, borrowing, or other types of transactions. Today's widespread use of relational and other databases to store transactions creates new opportunities to proactively search for fraud in businesses. In previous years, fraud audit techniques such as discovery sampling have been computerized to increase their efficiency. However, just as the computerization of traditional corporate processes at the dawn of the computer age did little to make those processes more effective (Hammer 1990), traditional fraud detection methods require a “business process reengineering” effort to fully utilize the power of modern computers and the large, rich data stores available to researchers.

2.2.1 Pre-emptive fraud investigation

A number of approaches to the assessment of fraud risk have been put forward in an attempt to enhance fraud detection by auditors. Some Arthur (1995) has suggested the use of pre-emptive fraud investigation which is a review intended to assess the vulnerability of an organization to
fraud. According to Sadgrove (2006) for such a review to be carried out successfully, one needs (a) to have adequate knowledge about both how fraud happens as well as about fraud indicators, and (b) to undertake a fraud vulnerability analysis of the company concerned. A vulnerability analysis assesses: what assets might be at risk; who might take them and who might benefit; how they might take them and sell them and, finally, how effective the controls are. Others Sorensen (1980) have proposed the use by auditors of the triangle model which comprises: (a) a strong, involved, investigative board of directors; (b) a sound, comprehensive system of internal controls; and (c) alert, capable independent auditors. The same authors also pointed out that if any of the points in the triangle do not function properly, the entire triangle will collapse, and the opportunity for management fraud is increased.

2.2.2 Log exceptions and to follow up

One of the most common ways to detect computer fraud is to log exceptions and to follow up on unusual activities in the logs. Exceptions that should be investigated include, for example: Transactions that are out of sequence, out of priority or otherwise out-of-standard; Aborted runs and entries, including repeated unsuccessful attempts to enter the system; Attempts to access applications or functions beyond a person's authorization level. If problems are uncovered, access logs and web activity logs may provide vital clues for tracking down the person involved. Some organizations implement logging, but only on a limited basis. Data may be refreshed or overwritten too frequently for the logs to be useful for gathering evidence at alter date. Logs should be maintained for at least a few months before being erased. Newly developed intrusion detection systems use artificial intelligence capabilities to detect unusual transactions flowing through a system. These are evolving and have the potential of providing an order- of magnitude improvement in crime detection technology.

Fraud detection includes both proactive and reactive activities targeted at finding the first indication that fraud might be occurring or undertaken to develop a “predication of fraud”. Most traditional fraud detection methods are reactive in nature that is, they are initiated by tips or complaints, control overrides, or other indicators that someone observes or hears. Proactive fraud
detection involves aggressively targeting specific types of fraud and searching for their indicators, symptoms, or red flags. Early fraud detection is critical because the sizes of most frauds increase geometrically over time as perpetrators gain confidence that their schemes are not being detected (Cortes et al., 2001).

Fraud examiners should follow up on all identified symptoms. While finding fraud is certainly the primary objective of follow up efforts, the process often highlights control weaknesses, ineffective systems, undocumented policies, and data errors. Each of these anomalies can be corrected to make company processes more efficient and effective. Follow-up not only involves eliminating control weaknesses and fixing system, but also involves dealing with perpetrators in ways that discourage future fraudulent acts (Albrecht, 2003).

The fraud detection process described thus far provides valuable information that helps investigators, auditors, and managers better understand a business and the types of frauds that could be occurring. After the cycle has been completed, the detection team should review what has been learned and determine how it can be improved. With greater understanding, new tools, and a set of tested algorithms, the strategic fraud detection process can be started again. Each of the subsequent process should be more efficient and effective than prior ones. The end result is a mature, tested process for detecting fraud and other anomalies.

Since much of the detection process is computerized, subsequent iterations are normally faster because analyses, algorithms, and models are already programmed. As analyses become more and more refined, they can be integrated directly into business processes. They can be programmed into new systems to stop problems at the time of data entry or transaction. They can be used to prevent anomalies before they occur (Webb, 2009).

In addition, detective measures can be run at specified periods automatically. They can be run against databases during off-peak hours to minimize their effect on corporate systems. Procedures can be programmed to highlight errors and send results to security personnel. For example, each week a different analysis could be run during the weekend and e-mailed to a corporate security team member for review on Monday morning (Provost and Fawcett, 2001).
2.2.3 Red flags approach

Other authors have proposed more specific methods for determining if fraud has occurred and is concealed in the financial statement. The widely-known red flags approach involves the use of a checklist of fraud indicators. The following examples of red flags are listed by Sadgrove: less physical stock in the warehouse than is shown by computer records; an employee suddenly gaining a lot of wealth, allegedly from an inheritance or a pools win and so forth; an employee who never takes a holiday; a supplier being given an undue amount of work or whose additional costs are accepted or who receives multiple orders at below the threshold for tendering unexplained credit notes; accounts that do not generate an invoice but are used for samples or guarantee claims.

It needs to be remembered, however, that red flags do not indicate the presence of fraud but represent conditions associated with fraud; in other words, they are cues meant to alert an auditor to the possibility of fraudulent activity, Porter (1993) which could have a material impact on the financial statement in a given circumstance. The use of red flags is recommended in textbooks on fraud detection and in auditing standards. The use of red flags questionnaires has three main advantages as a result of which one could reasonably expect them to increase the possibility of detecting fraud, namely raising the auditor’s sensitivity to the possibility of fraud, adding structure to the consideration of fraud, and providing consistency among auditors. A number of authors, however, have cast doubt on the predictive utility of red flags in fraud detection since they are plagued by two limitations: (a) while red flags are associated with fraud, the association is not perfect, and (b) since they focus attention on specific cues they might well inhibit the auditor from identifying or observing other reasons (Pinkus 1989).

2.2.4 Cognitive approach

According to Johnson et al (1993) the cognitive approach concerns itself with auditors’ thinking and reasoning that underlies their fraud-detection decision making. The cognitive approach has been used to detect fraud by utilizing information about an auditor’s expectations regarding the likelihood that fraud has occurred, and his/her degree of perceptual field dependence. The same
approach has also been used to detect fraud by enabling the auditor to think like the fraud perpetrator and thus avoid being fooled by the culprit’s deception tactics. According to Johnson et al.’s cognitive model, while management attempts to deceive the auditor by utilizing both their knowledge of the business and accounting practices as well as deep cognitive strategies and tactics (e.g. masking, double play, mimicking, dazzling, inventing, repackaging, decoying) and constructing a deception, auditors can use strategies and tactics (e.g anti-mimicking) for detecting such deceptions (Bernardi, 1994).

Fraud detection is becoming increasingly important to managers of organizations, to internal and external auditors, and to regulators. Fraud detection is an examination of the facts to identify the indicators of fraud sufficient to warrant recommending an investigation. In facts, there is no single test that a fraud has been committed. Most frauds involved an employee or manager of the victims’ organization. The most effective tools for fraud detection are internal audit review, specific investigation by management, employee notification and accidental discovery. Whistle-blowing is considered as another way of detection. Whistle-blower is the employee who reports unethical and illegal practices in the place of work. Whistle-blower needs to be protected and cherished by their employers (Vinten, 1994). Those who have an occasion in blowing the whistle are sometimes bitter about the results of having done so. Employee must be given an easy opportunity for whistle-blowing and must assure that it is okay to come forward (Vanasco, 2011).

In making the ordinary examination, an independent auditor is aware of the possibility that fraud may exist. Financial statements may be overstated as the result of defalcation and similar irregularities, or deliberate misrepresentation by management, or both. However, the ordinary examination in accordance with the auditing standards is directed to the expression of an opinion in financial statements and is not primarily or specifically designed to detect fraud. It cannot be relied upon to disclose the misstatement or omission, although their discovery may be fruitful at times.
2.2.5 Five-step fraud exposure approach

The five-step approach suggested by Vanasco (2011) for fraud detection in an audit is knowing fraud exposure in specific terms; knowing exposure specific symptoms of fraud; being alert for fraud symptoms; incorporating into routine audit program steps that are likely to reveal fraud symptoms; and following through on all observed symptoms.

Apostolou and Hassell (2000a) introduced fraud examinations as a non-recurring activity that was conducted when existence of a fraud in an organization was established. The main objective of the paper was to outline the differences between a fraud examination and a traditional audit. Fraud examination methodology was presented in the context of important legal considerations. It was a methodology of resolving fraud allegations from inception to disposition. Fraud examination involved obtaining evidence and taking statements, writing reports, and testifying to findings. The author stated that to conduct a fraud examination, the persons required skills to properly detect and investigate an allegation of fraud and also knowledge of the legal elements and which law to apply. The limitation is that she failed to fulfill her objective to elaborate how the traditional audit is different from the fraud examinations. In addition, it focused only on fraud examination and did not describe other preventive measures.

Benford’s law (Hill 2006) says that the distribution of the first significant digits of numbers drawn from a wide variety of random distributions will have (asymptotically) a certain form. Until recently, this law was regarded as merely a mathematical curiosity with no apparent useful application. However, Nigrini and Mittermaier (2011) and Nigrini (2009) show that Benford’s law can be used to detect fraud in accounting data. The premise behind fraud detection using tools such as Benford’s law is that fabricating data which conform to Benford's law is difficult. Fraudsters adapt to new prevention and detection measures, so fraud detection needs to be adaptive and evolve over time. However, legitimate account users may gradually change their behaviour over a longer period of time, and it is important to avoid spurious alarms. Models can be updated at fixed time points or continuously over time - see, for example (Senator, 2000).
2.2.6 Investigation approach

Investigation consists of performing extended procedures necessary to determine whether fraud, as suggested by the indicators, has occurred. It includes gathering sufficient evidential matter about the specific details of a discovered fraud. All computer fraud investigations need to start with a plan for gathering and handling the evidence. Internal auditors, lawyers, investigators, security personnel, and other specialists from inside or outside the organizations are the parties that usually conduct or participate in fraud investigations. The investigator must be familiar with good systems administration practices and possess extensive background of skills and knowledge relevant to computer security and various concepts at work in the areas under investigation (Wright, 2000).

When fraud has been detected, an organization’s main concern is to identify the source of fraud and to determine whether it is an internal or an external problem. According to the IIA Standards (SIAS No. 3), the roles of internal auditing in the investigation of fraud include: assessing the probable level and extent of the complexity of fraud within the organization; assessing the qualifications and the skills of the internal auditors and the specialists available to participate in the investigation to ensure that it is conducted by individuals having the appropriate type and level of technical expertise to effectively carry out the investigation; being cognizant of the rights of alleged perpetrators and personnel within the scope of the investigation and the reputation of the organization itself; designing procedures to follow in attempting to identify the perpetrators, extent of fraud, techniques used, and cause of fraud; and coordinating activities with management personnel, legal counsel, and other specialists as appropriate throughout the course of the investigation.

When a fraud investigation reveals irregularities, which may have an adverse impact on the financial position and results of operations, the internal auditors should inform the appropriate management and the audit committee. A suspect should not be confronted until supporting evidence has been gathered. Confrontation should be done by persons who specialize in investigating criminal activity, not by internal auditors.
2.2.7 Surveillance

Investigating a case may involve covert operations, surveillance, informants, dumpster diving and sources of information (Apostolou, 2000a). Covert (undercover) operations may be used to prove the allegation of fraud. The court deems the undercover operations, as an acceptable method of acquiring information, provided there is sufficient probable cause that a crime has been committed.

Surveillance is the secretive and continuous observance of a suspect's activities and is frequently used in developing evidence. It may be used to obtain probable cause for search warrants, develop investigative leads, identify co-conspirators, gather intelligence, and locate persons or objects. Informants are persons who have specific knowledge of a criminal activity. Informants can be extremely useful in fraud investigations regardless of their personal motivation for supplying information.

Dumpster diving is used when the investigator finds it necessary to sift a suspect's trash to obtain evidence and leads. Important documents and information concerning illegal activity may be found in garbage. The courts have upheld that investigators may sift through trash without a search warrant, provided that the trash has left a suspect's possession. After it has left the suspect's possession, there is no longer the reasonable expectation of privacy, and thus it is a fair game.

A large variety of information sources are available to the investigator to assist in the investigation of a case. Information can be “in-house” or public and might be used for locate individuals or verify their identity or research assets or financial positions or document lifestyles and background information.

2.3 Fraud Prevention Strategies

Fraud prevention procedures should have three realistic and measurable goals: reduce losses resulting from fraud; deter fraud through proactive policies; and increase the likelihood of early fraud detection. Fraud control policies should provide guidelines on ways to reduce the risk of
fraud. For example, a comprehensive security program assists in the prevention and detection of computer fraud from all sources. The use of various layers of properly implemented protection mechanisms will have the synergistic effect of increasing and enhancing a security program. Currently, many experts considered the “onion” model of security as the best and safest approach to manage the risks dealing with computer fraud (KPMG, 2001).

2.3.1 Internal control

The Accounting officer is ultimately held accountable for the design and implementation of a fraud prevention strategy and plan. It must further be emphasized that an understanding of overall risk (cumulative effect of inherent, control and detection risk) in relation to fraud risk is critical to the success of a fraud prevention plan. The value of internal control is apparent in both preventing and detecting fraud as prevention is better than cure. A weak internal control creates opportunities for fraud and about half of all frauds occur in the financial area (Vanasco, 2011). Internal control system has four broad objectives; those are to safeguard assets of the firm; to ensure the accuracy and reliability of accounting records and information; to promote efficiency in the firm's operation; and to measure compliance with management's prescribed policies and procedures (Havey, 2009). The effectiveness of internal control depends largely on management integrity.

The value of internal control is apparent in both preventing and detecting fraud as prevention is better than cure. A weak internal control creates opportunities for fraud and about half of all frauds occur in the financial area (Vanasco, 2011). Internal control system has four broad objectives; those are to safeguard assets of the firm; to ensure the accuracy and reliability of accounting records and information; to promote efficiency in the firm's operation; and to measure compliance with management's prescribed policies and procedures (Havey, 2009). The effectiveness of internal control depends largely on management integrity.
2.3.2 Deterrent security controls

Katz (2000) argued that maintaining security is a never-ending struggle. Just when one has an airtight system in place, a new hacker technology or an especially diabolical adversary enters the picture. A review of the literature, (Katz, 2000) reveals diverse views regarding the classification of CAIS security controls. Security controls of CAIS could be classified according to their purpose: to deter; to prevent; to detect; and to correct security threats.

The objective of deterrent security controls is to create an atmosphere of control compliance, while preventive security controls should be designed to reduce the possibility of an attack. Once a system has been violated, detective controls could help in identifying the occurrence of harm and security breach. Corrective controls serve to reduce the impact of the threat after a loss has occurred. Thus, the purpose of corrective controls is to aid in recovery from damage or in reduction of the harmful effects of its occurrence (Parker, 1981; Qureshi and Siegel, 2011).

Security controls could also be categorized according to their association with the data-processing stages into: input; processing; storing; and output security controls. The purpose of input controls is to ensure that each transaction is authorized, processed correctly and processed only once. Processing controls should be used to ensure that transactions entered into CAIS are valid and accurate, that external data are not lost or altered and that invalid transactions are reprocessed correctly. Output security controls are used to ensure that no unauthorized copies of output were made and that the printouts are directed only to authorized persons. Storage security controls ensure that all stored data and programs are secured against unauthorized access, manipulation, alteration and disclosure. Alternatively, security controls could also be classified according to their nature, including, for example, organizational, physical access, data and data integrity, software, off-line programs and data security controls.

Von Solms (2006) has addressed the general background about security evaluation. He discussed the scope of information security and the responsibility for information security. A number of information security evaluation schemes and certification techniques, such as trusted security evaluation criteria schemes,
The cost of a fraud is not only a monetary loss, but it vitiates the organization’s atmosphere, creates mistrust and calls for harsh measures that could have been avoided. Reviewing and improving internal control are often thought of as the primary defense against fraud and abuse. A strong system of internal control is the most effective method of fraud prevention. Prevention of fraud starts with identification of the weakness in the current systems of an organization. Next, the organization must improve those systems with new or better controls. The introduction and enforcement of controls will reduce the opportunities for fraud. The control warns potential fraudsters that management is actively monitoring the business and that in turn deters fraud. As a result, an organization, which seeks to contain computer fraud, should strive to implement a broad range of interventions, be it technical, formal or informal. Technical interventions are controls implemented to limit access to building, rooms or computer systems. Formal interventions involve horizontal expansion of the hierarchy of organization to have a flatter pyramid. Education, training and awareness programmes are some measures implemented in the informal interventions. Controls have dysfunctional effects because isolated solutions have been provided for specific problems. These “solutions” tend to ignore other existing controls and their contexts. Thus, individual controls in each of the three categories, though being important, must complement each other. This necessitates an over-arching policy, which determines the nature of controls being implemented, and therefore provides a comprehensive security to the organization (Baker, 2009).

2.3.3 Employees approach

Employees have the highest possibilities to be fraudsters. Thus, the main factor which fraud can be contained lies in ensuring that trustworthy and reliable staffs are employed, particularly in positions of responsibility (Vanasco, 2011). Employee has the ability to make use of confidential information or facilities to commit fraud or collude with an outsider to perpetrate a crime. Performing background checks, to a certain extent, would help to prevent fraud. The level of background checks performed should be commensurate with the level of risk associated with the position (KPMG, 2001).
The best way of preventing fraud is to understand why it happened. Fraudsters generally identify an opportunity for exploiting a weakness in the control procedures and then assess whether their potential rewards would outweigh the penalties should they be caught. In addition, the paper introduced the two-stage processes of fraud prevention. First, an organization must ensure that opportunities for fraud were minimized: fraud prevention. Second, organization should ensure that potential fraudsters believe they will be caught: fraud deterrence. Introduction and enforcement of new controls would reduce the opportunities for perpetrators. A regular control was most effective and normally required little management time or effort. It also emphasized the importance of having strong management and a healthy corporate culture to detect and consequently deter fraud. The limitation of this paper is that it did not specify the detailed control procedures for two-step processes of fraud prevention. It failed to explain the financial effects and risk of computer fraud if prevention and deterrence procedures were not in place.

2.3.4 Managerial framework

Boomer (2007) discussed the designation of a managerial framework to control the operational risk, and focus on unauthorized trading fraud. A sample of 37 cases was taken for examination from financial institutions in eight countries over the period 2008-2009. The sample results indicated that internal controls were the primary defense against severe fraud losses and showed that the regulatory penalties imposed on senior supervisory management, in addition to the fraudster, were crucial in ensuring efficient mitigation of fraud loss. Losses from unauthorized trading fraud can be identified with breakdown of controls and constraints designed to mitigate losses from operational risk. The limitation of the paper is that only one type of fraud was analyzed, as there may be other types of fraudulent activities in the financial services industry. The survey also failed to identify the motives of fraud and other preventive measures to combat fraud.

Vanasco (2011) emphasized that fraudulent financial statements were a great concern to the corporate world and the accounting profession. In particular, the author examined the roles of professional associations, governmental agencies and international accounting and auditing
bodies in promulgating standards to deter and detect fraud in the US and a few other countries. Vanasco also examined the impact of management and employee fraud on various business sectors, government bodies and non-profit entities. He discussed the roles of management, the board of directors, the audit committees, auditors, and fraud examiners as well as their liabilities in fraud prevention and investigation. The author explained the ideal control environment to prevent fraud and also focused on the techniques and preventive procedures in the investigative and reporting process. In addition, the writer elaborated on white-collar crimes constituting employee fraud, embezzlement, kiting, larceny, lapping and pilferage. Vanasco also noted several accounts in the financial statements that are vulnerable to fraud. The limitation of the paper is that it did not focus on the impact of fraud on accounting transactions and financial statements. It failed to measure the effect of fraud to victims in monetary terms and the psychological impact on the morale of the employees.

2.3.5 Auditor approach

Moyes and Hasan (2006, p. 46) concluded that the degree of fraud detection was not dependent on the type of auditor, since both internal and external auditors have equal abilities to detect fraud. Moyes and Hasan (2006, p. 46) also found that organizational success in detecting fraud was significantly enhanced in auditing firms with previous experience in fraud detection than auditing firms with no such history. It was also found that auditors who were certified as certified public accountants (CPAs) were more likely to detect fraud than auditors who were non-CPAs. Moyes and Hasan (2006) argued that this certification may imply a greater level of professional competence in fraud detection. The authors further argued that the peer review process puts pressure on auditors to be more diligent in incorporating relevant audit procedures to detect fraud.

Bonner et al. (2011) concluded that there existed some support for higher incidence of litigation against auditors, when a company's financial statements contain fraud that most commonly occurs, or when fraud arises from fictitious transactions and events. Summers and Sweeney (2011) found that insiders reduced their equity stake during the occurrence of fraud.
Colbert (2000) illustrated how the International Federation of Accountants and the American Institute of Certified Public Accountants provided guidance to auditors for detecting misstatements in the financial statements that were caused by errors and fraud. Misstatements may be the result of error or fraudulent activities. The author made the comparison of International Standard for error and fraud to the two US audit Standards and disclosed several similarities and few differences particularly on reassuring to auditors serving client offering cross-border securities. The major provisions in the standards provided guidance related to the definitions of error and fraud, the categories of risk, the process of assessing risk, and recommended audit procedures performed to locate and report errors, were alike. She further concluded that the remarkable consistency between the Standards implied that, comparable work was being performed no matter which guidance the auditor was utilizing. The limitation is that the paper only provides guidance from the point of view of the auditors; and did not provide a platform for fraud prevention procedures that could be carried out by management. Despite the differences noted in comparing the standards, no recommendation for improvement or amendment to standards was made to the less well development standards.

Farrell and Franco (2009) conducted a survey objectively to determine the variation in the opinion of those working for the former “Big Six” and other accounting firms. The survey was based on questionnaires mailed to approximately 1,700 accounting firms in New York, New Jersey and Connecticut areas, and approximately 300 questionnaires to the former “Big Six” accounting firms in the United States. The interviewees were mainly managers and partners with only 10 per cent response rate. They concluded from the survey that all organizations were victimized by high product costs and low corporate profits. Normally everyone gets shock and disbelief when fraud was detected within an organization. They also stress the motives and specific characteristics of the offenders and the importance of prevention or detection strategies against business fraud. The auditor played an important role in prevention and detection of business fraud. The limitation of this paper is that the samples of the survey were only limited to certain areas of the United States. Moreover, the response rate may be too low to represent the whole population. The generality of the empirical findings are therefore dubious.
2.3.6 Risk assessment

McNamee (2009) introduced risk assessment as a tool to help to detect and deal with fraud in operations of organizations. He emphasized that managers had to take responsibilities to locate fraud. Risk assessment could also be used as a decision-making tool to assist managers sort through a number of possibilities and single out those with the greatest payoff. Furthermore, managers could use this technique to identify and prioritize the most likely business processes where potential fraud could occur. McNamee further analyzed the three elements of risk assessment. First is risk identification to determine the high-risk areas and its sources. Secondly, risk measurement to determine the consequences of the risk and likelihood of its occurrence. Last, risk prioritization is to determine the appropriate resources to manage the risk. This paper only focused on one particular tool to detect fraud and did not suggest any alternative. It failed to give examples to illustrate the application of the tool to investigate fraud.

Coffin (2003) introduced the approaches adopted by auditors in deriving an audit strategy. The two approaches were procedures-driven approach and the risk-driven approach. Procedures-driven approach did not make full consideration of the risk present. In this approach, the auditor determined the specific audit procedures to be performed without considering the objective of the related risk. This approach involved assessing, during planning period, the various risks in each area. Generally, risk-driven approach was more effective and efficient than the procedures-driven approach because risk-driven approach focused on the internal auditor's effort areas with relatively more risk. The limitation of the paper is that it did not address the risk factors of an engagement on the procedures-driven approach. The authors failed to discuss in detail how the risk-driven approach helps detection of fraud.

Riahi-Belkaoui and Picur (2000) stated that organizations today were more susceptible to fraud in the accounting environment than ever before. Fraud had caused massive losses to firms, individuals and society. They presented a general framework that was useful to identify conditions that were most conducive to fraud in the accounting environment. The framework was based on models and theories from criminology including conflict and consensus approaches, the
ecological theory, cultural transmission theory and anomie theory. These theories offered alternative explanations for corporate fraud, white-collar crime, fraudulent financial reporting and audit failures. The authors failed to provide the steps on how to use the framework to categorize the fraud perpetrated in the accounting world. The paper also failed to mention the detective and preventive procedures that can be implemented.

The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. Because of the nature of audit evidence and the characteristics of fraud, the auditor is able to obtain reasonable, but not absolute, assurance that material misstatements are detected. The auditor has no responsibility to plan and perform the audit to obtain reasonable assurance that misstatements, whether caused by errors or fraud, that are not material to the financial statements are detected (Arens et al., 2003, p. 138).

Apostolou (2000c) provided background information for enhanced understanding of occupational fraud and abuse. The responsibilities of auditors and fraud examiners were also highlighted. She explained the fundamentals of fraud, which consist of the typical schemes, legal elements of fraud, detection and prevention techniques. By referring to the statistical finding in “2002 Report to the Nation on Occupational Fraud and Abuse”, she noted that the fraud and abuse cost organizations an estimated $400 billion losses annually. The author further categorized fraud into fraudulent financial reporting (management fraud) and misappropriation of assets (employee fraud). Examples were quoted from the professional standards, and risk factors of management fraud were analyzed into: management's characteristics and influence over its control environment; industry conditions; and operating characteristics and financial stability.
2.4 Fraud Related Risks Responses Improvement Strategies

2.4.1 Corporate strategy planning

Fraud risk should be included on the agenda of every corporate strategy planning meeting; it should be raised at main Board level on a frequent and regular basis. Systems and controls should be examined to identify weaknesses which make the company susceptible to the risk of fraud. Employment and recruitment practices should be scrutinized, to ensure that only those new recruits to the business whose references have been taken up and checked thoroughly are employed; that existing staff are surveyed regularly, if unobtrusively, by HR, to monitor their taking of leave, their use of corporate credit cards, their own lifestyles, where this is possible. Many lower paid staff is enjoying a startlingly extravagant private life, with sumptuous houses, cars and mistresses, well known to their colleagues, but often hidden from senior management. Line managers should not be coy about asking the pertinent question, if there is evidence that a staff member is apparently living well above his or her means.

Misstatements arising from fraudulent financial reporting are intentional misstatements or omissions of amounts or disclosures in the financial statements to deceive users (AICPA, 2011b). Misstatements arising from the misappropriation of assets involve the theft of an entity’s assets (AICPA, 2011b). Misappropriation of assets is typically accomplished by embezzling receipts, stealing, or causing an entity to pay for goods or services not received and accounts for more than four out of five fraud offenses (ACFE, 2006). Concealment is the key attribute that distinguishes fraud from other criminal acts such as sabotage, arson, extortion, etc. (ACFE, 2006; Albrecht et al., 1995). This category of fraud is most often perpetrated by employees rather than management (Wells, 2011).

According to Cressey (2007), a nonsharable financial need is crucial to understanding the behaviour of one who violates a trust to commit fraud. What is deemed nonsharable is in the eyes of the offender (Cressey, 2007). These “nonsharable” needs are divided into six basic types: violation of ascribed obligations, problems resulting from personal failure, business reversals,
physical violation, status gaining, and employer-employee relations (Cressey, 2007). Cressey’s model helps explain the nature of many, but not all occupational offenders (Wells, 2011).

2.5.2 Fraud control framework

Sound prevention strategies are the foundation of a reliable fraud control framework. While they cannot eliminate fraud risk, coordinated and effectively implemented strategies can minimise the chances of it occurring. Key preventative measures critical to a sound fraud control framework include: a fraud control plan documenting the responsibilities for fraud prevention, detection and response initiatives; periodic fraud risk assessments to identify and treat major fraud risks, and inform the fraud control plan; a fraud policy establishing clear standards and procedures for dealing with suspected fraud incidents; a code of conduct clarifying the council’s expectations for ethical behaviour that is demonstrably adhered to and promoted by senior management; regular staff fraud awareness training on their responsibilities for identifying, preventing and reporting potential wrongdoing; scrutiny by internal audit and the audit committee of the effectiveness of the council’s fraud control framework and related activities; and effective controls for activities with a high fraud risk exposure. Once implemented, these preventative measures should be regularly monitored and evaluated to assure their effectiveness in operation.

2.5.3 Refresher training for staff

Induction and periodic refresher training for staff assists in assuring they are aware of and understand their fraud control responsibilities. Further, periodic evaluations of a banks fraud control arrangements are important for continuous improvement and for assuring they remain effective. Specifically, they can assist in determining: the relevance and priority of fraud strategies in light of current and emerging risks; whether fraud strategies are effectively targeting the right and/or desired areas; and whether there are more cost-effective ways of managing key fraud risks. They should also assess and where necessary strengthen their internal controls to efficiently and effectively mitigate their fraud risks.
Research by KPMG indicates that more than half of all major frauds occur because of poor internal controls or the overriding of these controls. Adequate internal control systems are critical for preventing and detecting frauds. According to KPMG (2011), the banks should: develop and maintain an up-to-date fraud control plan clearly documenting their fraud prevention, detection and response initiatives and responsibilities; conduct thorough, periodic fraud risk assessments to assure they identify and effectively manage all major fraud risk exposures; provide induction and periodic fraud awareness training to all council staff, to assure they understand their fraud control responsibilities; systematically monitor and report on the effectiveness of their fraud control strategies; and establish arrangements that assure effective ongoing scrutiny by executive management, internal audit and audit committees, of the effectiveness of the fraud control framework.

2.5.4 Quality of staff

To improve the control system, the banks should: establish effective pre-employment screening processes that provide sufficient assurance over the integrity, identity and credentials of all council staff; make sure accounts payable systems have effective preventative and/or compensating controls that adequately mitigate the risk of fraudulent purchases and/or payments; maintain accurate and an up-to-date asset registers that are regularly reviewed to mitigate the misuse and/or misappropriation of assets; and systematically review the operation and effectiveness of all their internal control systems to assure they adequately prevent, deter and detect major frauds.

In order to develop and implement a Fraud Prevention Strategy, the banks need to identify where exposures to fraud exist within the Institution’s current operating systems and procedures. Only once these exposures have been identified will it be possible to implement action to counter the exposures and, wherever possible, prevent or reduce the incidence of fraud in the future.

All employees are responsible for the management of fraud risk, to some extent, but the Accounting Officer / Authority has the ultimate responsibility. The Accounting Officer / Authority can delegate the responsibility to line managers in specific areas of the Institution. The
Accounting Officer / Authority can delegate responsibility of fraud risk management along with the flow of activities from strategic to operational level. As part of the response plan the Institution should develop clear procedures on how to address controls deficiency. The Institution should develop clear lines of reporting fraud. Fraud reporting should be part of the response plan or investigation policy. The response plan should also outline the activities and the personnel responsible for specific response activities.

The legislation that is relevant to addressing civil and criminal acts against the Institution should be outlined and clearly interpreted. It should be clear what constitutes the act of fraud and/or corruption. The Accounting Officer/Authority should put structures in place to promote and educate the stakeholders about the Institution’s culture on fraud and corruption. Management can be charged with responsibility of training other employees under their supervision, on fraud and corruption, as part of anti-fraud programme.

2.5 Chapter Summary

This chapter reviews the relevant literature in relation to the research questions presented in the study. The discussion tackles all the research objectives posed and provides a firm theoretical background for the study. The chapter discusses how banks respond to the teething fraud risk problem using a theoretical and empirical review.

The next chapter; Research Methodology, presents the research design, data collection methods, and how results were analyzed in the study.
CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

This chapter sets out various stages and phases that were followed in completing the study. It involves a blueprint for the collection, measurement and analysis of data. This section is an overall scheme, plan or structure conceived to aid the researcher in answering the raised research question. In this stage, most decisions about how research was executed and how respondents were approached, as well as when, where and how the research was completed. Therefore in this section the research identifies the procedures and techniques that were used in the collection, processing and analysis of data. Specifically the following subsections are included; research design, target population, data collection instruments, data collection procedures and finally data analysis.

3.2 Research Design

Research design refers to the overall plan used to carry out a research. This research problem was studied through the use of a descriptive survey design. According to Cooper and Schindler (2007), a descriptive survey design is concerned with finding out the what, where and how of a phenomenon. According to Chandran (2004), a descriptive survey design is concerned with gathering facts or to obtain pertinent and precise information concerning the current status of phenomenon and whatever possible to draw possible conclusions from the facts discovered. It is concerned with the generalized statistics that result when data are abstracted from a number of individual cases (Zikmund, 2009).
3.3 Population and Sampling Design

3.3.1 Target Population

Target population for in statistics is the specific population about which information is desired. According to Ngechu (2004), a population is a well defined or set of people, services, elements, events, group of things or households that are being investigated. The target population of this study was the management staff working at commercial banks headquarters in Nairobi. The study focused particularly on the top, middle and lower level management staff who are directly dealing with the day to day management of the banks since they are the ones conversant with the subject matter of the study. So the researcher intended to examine a sample of staff drawn from the population of 597 management staff working in commercial banks of the top, middle and low level management ranks at the headquarters in Nairobi. Mugenda and Mugenda (2003), explain that the target population should have some observable characteristics, to which the researcher intends to generalize the results of the study. The population is as summarized in the table below.

Table 3.1: Target Population

<table>
<thead>
<tr>
<th>Category</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior managers (‘P’ and above)</td>
<td>44</td>
<td>9.7%</td>
</tr>
<tr>
<td>Middle level managers (‘M’ and ‘N’)</td>
<td>185</td>
<td>28.6%</td>
</tr>
<tr>
<td>Low level managers (‘A’ – ‘L’)</td>
<td>368</td>
<td>61.6%</td>
</tr>
<tr>
<td>Total</td>
<td>597</td>
<td>100%</td>
</tr>
</tbody>
</table>

Source: Banks HR records, 2012

3.3.2 Sample Design

3.3.2.1 Sampling Frame
The sampling frame describes the list of all population units from which the sample was selected (Cooper and Schindler, 2007). Ngechu (2004) underscores the importance of selecting a representative sample through making a sampling frame. From the population frame the required number of subjects, respondents, elements or firms were selected in order to make a sample.

### 3.3.2.2 Sampling Technique

Stratified proportionate random sampling technique was used to select the sample. According to Babbie (2004) stratified proportionate random sampling technique produce estimates of overall population parameters with greater precision and ensures a more representative sample is derived from a relatively homogeneous population. Stratification aims to reduce standard error by providing some control over variance. The study group the population into three strata i.e. senior managers, middle level managers and low level managers. From each stratum the study used simple random sampling to select 234 respondents. Statistically, in order for generalization to take place, a sample of at least 30 elements (respondents) must exist (Cooper and Schindler, 2007). Kothari (2010) also argues that if well chosen, samples of about 10% of a population can often give good reliability and so 30% was even better.

### 3.3.2.3 Sample Size

A sample size of 234 was arrived at by calculating the target population of 597 with a 95% confidence level and an error of 0.05 using the below formula taken from Mugenda and Mugenda (2003):

From Normal distribution the population proportion can be estimated to be

\[ n = \frac{Z^2 PQ}{\alpha^2} \]

Where:

- \( Z \) is the Z – value = 1.96
P Population proportion 0.50

\[ Q = 1 - P \]

\[ \alpha = \text{level of significance} = 5\% \]

\[ n = \frac{1.96 \times 1.96 \times 0.5 \times 0.5}{0.05 \times 0.05} \]

\[ n = 384 \]

Adjusted sample size

\[ n.' = \frac{384}{1 + (384/597)} \]

\[ \text{Approx} = 234 \]

The selection was as follows.

**Table 3.2: Sample Size**

<table>
<thead>
<tr>
<th></th>
<th>Total population</th>
<th>Percentage</th>
<th>Sample size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior managers (‘P’ and above)</td>
<td>44</td>
<td>0.39</td>
<td>17</td>
</tr>
<tr>
<td>Middle level managers (‘M’ and ‘N’)</td>
<td>185</td>
<td>0.39</td>
<td>72</td>
</tr>
<tr>
<td>Low level managers (‘A’ – ‘L’)</td>
<td>368</td>
<td>0.39</td>
<td>144</td>
</tr>
<tr>
<td>Total</td>
<td>597</td>
<td>0.39</td>
<td>234</td>
</tr>
</tbody>
</table>

**Source:** Research, (2013)
3.4 Data Collection

The study was collected both primary and secondary data. Primary data was collected using a questionnaire while secondary data was obtained from annual reports of the companies.

This research utilized a questionnaire for primary data collection. The questionnaire designed in this study comprised of two sections. The first part included the demographic and operational characteristics designed to determine fundamental issues including the demographic characteristics of the respondent while the second part dealt with the study variables.

3.5 Research Procedure

This study collected quantitative data using a self-administered questionnaire. The researcher dropped the questionnaires at the respondents’ place of work. Nevertheless, where it proves difficult for the respondents to complete the questionnaire immediately, the researcher left the questionnaires with the respondents and pick them up later. The structured questions were used in an effort to conserve time and money as well as to facilitate in easier analysis as they are in immediate usable form; while the unstructured questions were used so as to encourage the respondent to give an in-depth and felt response without feeling held back in revealing of any information. Each questionnaire was coded and only the researcher knew which person responded. The coding technique was only used for the purpose of matching returned, completed questionnaires with those delivered to the respondents. Secondary data was corrected from already documented materials such as the banks’ annual reports, banking survey report, journals and periodicals.

The researcher w carried out a pilot study to pretest the validity and reliability of data collected using the questionnaire. According to Creswell (2003), validity is the degree by which the sample of test items represents the content the test is designed to measure. Content validity which was employed by this study is a measure of the degree to which data collected using a particular instrument represents a specific domain or content of a particular concept. Mugenda and Mugenda (2003) contend that the usual procedure in assessing the content validity of a
measure is to use a professional or expert in a particular field and hence professional advice was sought from lecturers in the Department of Accounting and Finance including the supervisor.

According to Babbie (2004), reliability refers to the consistency of measurement and is frequently assessed using the test–retest reliability method. Reliability is increased by including many similar items on a measure, by testing a diverse sample of individuals and by using uniform testing procedures. The researcher selected a pilot group of 20 individuals from the target population of the staff working in commercial banks to test the reliability of the research instrument. The pilot study allowed for pre-testing of the research instrument. The clarity of the instrument items to the respondents necessary so as to enhance the instrument’s validity and reliability. The aim was to correct inconsistencies arising from the instruments, which ensured that they measure what is intended. The pilot data was not be included in the actual study.

3.6 Data Analysis

Data analysis is engaged in after all data has been collected and is a process used to make sense of the data. The type of data analysis tool that would be used is dependent on the type of data, that is; is the data qualitative or quantitative (Walsh and Wigens, 2003). Before processing the responses, the completed questionnaires were edited for completeness and consistency. The data was then coded to enable the responses to be grouped into various categories. Data categorizations ensured appropriateness, exhaustiveness, mutual exclusivity and have a single dimension or the use of one concept. Data collected was purely quantitative and it was analyzed by descriptive analysis including the mean, standard deviation, frequencies and percentages. The statistical tools such as SPSS and MS Excel helped the researcher to describe the data and determine the extent used. The use of structured questionnaires enabled the researcher to quantify quantitative data using the size, frequency distribution, and association of variables in the study population and answers to questions that could be counted and expressed numerically. Tables and figures were used to summarize responses for further analysis and facilitate comparison. In addition, the researcher conducted a multiple regression analysis so as to determine the effects of each of the four variables on performance of the banks. Regression was
used to estimate the coefficients of the linear equation, involving one or more independent variables, which best predicted the value of the dependent variable

Voluntary participation all that participated was not coerced into participating in the research as the researcher wrote notifications in advance for any of the participant’s thus promoting informed consent for all that was involved. The researcher ensured that guarantees to the participants concerning confidentiality are given and strictly observed. Information was not be made available to anyone who is not directly involved in the study. The strict standard of anonymity was employed which meant that the participant remained anonymous throughout the study even to the researchers themselves. Other ethical issues that were put in check include; Honesty: The researcher strived to maintain truthfulness in reporting data results by ensuring that there is no fabrication, falsehood, or any misrepresentation of data. Objectivity: The researcher avoided bias in experimental design, data analysis, data interpretation, peer review, and expert testimony among others. Carefulness: The researcher ensured that careless errors and negligence are avoided as good records of research were kept such as data collection and research design. Respect for Intellectual Property: The researcher honored patents, copyrights, and other forms of intellectual property by accrediting and acknowledging of contributions from various parties. Confidentiality: Confidential communications, such as customer and workers records was kept in confidence. Non-Discrimination: The researcher avoided discrimination against colleagues or customers on the basis of sex, race, ethnicity, or other factors that are not related to their scientific competence and integrity.

3.8 Chapter Summary

This chapter presents the research methodology that was used for this study. The chapter covers research design, population and sampling design, data collection methods, research procedures, data analysis methods. The next chapter presents the results and findings of the study.
CHAPTER FOUR

4.0 RESULTS AND FINDINGS

4.1 Introduction

This chapter presents analysis and findings of the study as set out in the research methodology. The results are presented on the responses by commercial banks in Kenya to fraud related risks in the industry. The data was gathered exclusively from questionnaire as the research instrument. The questionnaire was designed in line with the objectives of the study. To enhance quality of data obtained, Likert type questions were included whereby respondents indicated the extent to which the variables were practiced in a five point Likerts scale.

4.1.1 Response Rate

The study targeted to sample 234 respondents in collecting data. From the study, 180 out of 234 sampled respondents filled in and returned the questionnaire contributing to 76.9%. This commendable response rate was made a reality after the researcher made personal calls and visits to remind the respondent to fill-in and return the questionnaires.

Table 4.1: Response Rate

<table>
<thead>
<tr>
<th>Response</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responded</td>
<td>180</td>
<td>76.9</td>
</tr>
<tr>
<td>Not responded</td>
<td>54</td>
<td>23.1</td>
</tr>
<tr>
<td>Total</td>
<td>234</td>
<td>100.0</td>
</tr>
</tbody>
</table>
4.2 General Information

The study sought to find out the gender of the respondents.

![Pie chart showing gender distribution]

Figure 4.1: Gender of the respondents

On the gender of the respondents, the study found that there were more males as shown by 62.2% than females shown by 37.8% of the respondents.

The respondents were requested to indicate their age.
From the study findings, majority of the respondents (35.1%) were between 41 – 44 years, 32.4% were between 35 – 40 years, 13.5% were between 45 – 50 years, 10.8% were between 31 - 34 years, 5.4% were between 25 - 30 years while a small proportion of the respondents (2.7%) were over 51 years old.

The respondents were also requested to indicate the number of years that they had been working with the bank

![Bar chart showing duration served in the Commercial banks](image)

**Figure 4.3: Duration served in the Commercial banks**
According to the study, most of the respondents as shown by 64.9% reported that they had been working with the bank for a period of 6 to 10 years, 21.6% of the respondents had worked with the bank for a period between 2 – 5 years, 10.8% said 11 years and more, while 2.7% of the respondents said that they had worked with the bank for less than 2 years.

The study sought to find out the highest level of education of the respondents.

![Figure 4.4: Highest level of education](image)

The study found that the majority of respondents (48.6%) had a Bachelors degree as their highest level of education, followed by 21.6% who had a Masters degree, 16.2% who had a Higher National Diploma, 8.1% who had professional qualification (CPA, CFA) while those who had a PhD or Diploma were represented by 2.7%.

41
4.3 Fraud Detection

The study sought to establish whether there are fraud detection strategies adopted by commercial banks in Kenya. From the study findings, majority of the respondents (73%) indicated that there are fraud detection strategies adopted by commercial banks in Kenya while 27% of the respondents differed with this.

Table 4.2: Whether there are fraud detection strategies adopted by Commercial Banks in Kenya

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>131</td>
</tr>
<tr>
<td>No</td>
<td>49</td>
</tr>
<tr>
<td>Total</td>
<td>180</td>
</tr>
</tbody>
</table>

The study sought to investigate the extent that fraud detection strategies are adopted at the Commercial banks. According to the study findings, 48.6% said that fraud detection strategies are adopted at the Commercial banks to a very great extent, 29.7% said to a great extent while 21.6% of the respondents said to a moderate extent.

Table 4.3: Extent that fraud detection strategies are adopted at the Commercial banks

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very great extent</td>
<td>87</td>
</tr>
<tr>
<td>Great extent</td>
<td>53</td>
</tr>
<tr>
<td>Moderate extent</td>
<td>39</td>
</tr>
<tr>
<td>Total</td>
<td>180</td>
</tr>
</tbody>
</table>
The study sought to investigate the extent that the respondents employ various fraud detection strategies in Commercial banks. A 5-point likert scale was used where 1-1.499=not at all; 1.5-2.499=low extent; 2.5-3.499=moderate extent; 3.5-4.499=great extent and 4.5-5.0=very great extent.

From the study, the banks employed specific investigation by management, forensic investigation, HR / disciplinary procedures and internal audit reporting & security to a great extent as shown by a mean of 4.440, 4.237, 4.204 and 4.086 respectively. In addition, the banks employed employee notification, use of informants and reviewing, analyzing the causes of fraud and error and fraud audit program to a great extent as shown by a mean of 4.041, 3.980, 3.980 and 3.960 respectively. Moreover, the banks employed estimating the extent of fraud and error within the system, using technology to gather data about symptoms, use of surveillance and tip-offs to a great extent as shown by a mean of 3.920, 3.901, 3.740 and 3.729 respectively. The banks also employed computer imaging and analysis and data mining tools, internal audit review, use of external sources of information, security / audit investigations and line management to a great extent as shown by a mean of 3.720, 3.701, 3.571, 3.531 and 3.508 respectively. The banks employed use of covert operations and whistle-blowing to a moderate extent as shown by a mean of 3.449 and 2.980 respectively.

Fraud detection is an examination of the facts to identify the indicators of fraud sufficient to warrant recommending an investigation. In facts, there is no single test that a fraud has been committed. Most frauds involved an employee or manager of the victims' organization. The most effective tools for fraud detection are internal audit review, specific investigation by management, employee notification and accidental discovery. Whistle-blowing is considered as another way of detection. Whistle-blower is the employee who reports unethical and illegal practices in the place of work.

The study sought to investigate the capacity and functionality of fraud investigation strategies adopted by commercial banks in response to fraud risks. The interviewees indicated that fraud management in the bank is anchored on 5 key departments which include Compliance, Risk and
Advisory services (RAS), Control and Governance (C&G), Internal Audit (IA) and Security and Investigations Services & Fraud Management (SIS & FM). All the departments work jointly as a team towards eradicating fraud. The Compliance department deals with issues of account opening screening, due diligence on vendors and AML. They also implement group sanctions. RAS is charged with carrying out risk tests on all new products that are to be introduced into the market. They carry out assessments on new and existing products to identify any loop holes that fraudsters can use to siphon money out. They ensure that sufficient controls are in place for new products to be rolled out. They also carry out continuous checks for existing products in the market to ensure that they updated in line with any changes in the operating environment. BIA is the internal Audit function of the bank. Its role is to check whether requisite procedures are in place and are followed. Control & Governance department is a retail function that takes care of all control issues in the retail outlets (branches). The department is structured into regions headed by Senior Control Managers and their work is to ensure that control procedures are followed. SIS & FM is a Head office department. Its core function is advice on security matters, offer fraud training and carry out investigations. All cases are reported into the department for action. The department reports directly into the COO to insulate it from unnecessary influence. The team is charged with enforcing the Group Fraud Policy. It makes recommendation to the Group Chief Executive of Financial Crimes.

Table 4. 4: Extent that the respondents employ various fraud detection strategies in commercial banks

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal audit review</td>
<td>3.701</td>
<td>0.953</td>
</tr>
<tr>
<td>Specific investigation by management</td>
<td>4.440</td>
<td>0.611</td>
</tr>
<tr>
<td>Employee notification</td>
<td>4.041</td>
<td>0.947</td>
</tr>
<tr>
<td>Use of Surveillance</td>
<td>3.740</td>
<td>1.209</td>
</tr>
<tr>
<td>Use of Informants</td>
<td>3.980</td>
<td>1.315</td>
</tr>
<tr>
<td>Use of external Sources of information</td>
<td>3.571</td>
<td>1.099</td>
</tr>
<tr>
<td>Use of Covert operations</td>
<td>3.449</td>
<td>1.243</td>
</tr>
<tr>
<td>Tip-offs</td>
<td>3.729</td>
<td>1.041</td>
</tr>
</tbody>
</table>
4.4 Fraud Prevention

The study sought to investigate whether there are fraud prevention strategies adopted by commercial banks. From the study findings, majority of the respondents (78.4%) indicated that there are fraud prevention strategies adopted by commercial banks while 21.6% of the respondents differed with this.

Table 4.5: Whether there was fraud prevention strategies adopted by commercial banks

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>141</td>
</tr>
<tr>
<td>No</td>
<td>39</td>
</tr>
<tr>
<td>Total</td>
<td>180</td>
</tr>
</tbody>
</table>
The study sought to investigate the extent are fraud prevention strategies adopted by the bank. According to the findings, 85% of the respondents indicated that the banks adopted fraud prevention strategies to great extent, 10% of the respondents indicated that the banks adopted fraud prevention strategies to a very great extent and 5% of the respondents indicated that the banks adopted fraud prevention strategies to a moderate extent.

![Bar chart showing the extent of fraud prevention strategies adopted by the bank]

**Figure 4.5: Extent that fraud prevention strategies adopted by the bank**

The study sought to find out the extent that the aspects of fraud prevention strategies were adopted by the banks. From the findings, certification of auditors, creating internal audit departments (creation of anti-fraud culture / behaviours) and implementing internal controls & compliance were adopted in the bank to a great extent as shown by a mean of 4.917, 4.708 and 4.680 respectively. In addition, ensuring staff involved in the administration of benefit are adequately trained and maintain the highest, standard of probity – including completion of staff declaration, staff training and development, risk identification & assessment (identifying areas that are susceptible to abuse and make recommendations with regard to making systems more secure), deterrent security controls and adopting robust processes for verifying claims were adopted in the bank to a great extent as shown by a mean of 4.486, 4.469, 4.131, 4.021 and 3.837 respectively. Moreover, raising customer awareness about requirement to report changes, pre-
employment screening, evaluating defences and adjusting them in the light of experience, simplifying the claim process (system thinking in delivery of benefit service) and maintaining an accurate and complete asset register with clear asset descriptions were adopted in the bank to a great extent as shown by a mean of 3.021, 2.901, 2.861, 2.804 and 2.720 respectively. The respondents indicated that peer review process, designing corporate fraud policies (anti-fraud programmes), monitoring and evaluating various proactive initiatives and following up on suspected frauds (Referring suspicious cases to the fraud teams) were adopted in the bank to a great extent as shown by a mean of 2.380, 2.319, 2.229, 2.212 and 2.072 respectively. The respondents also indicated that publicizing fraud occurrences and whistle-blower systems were adopted in the bank to a great extent as shown by a mean of 1.820 and 1.260 respectively.

Table 4.6: Extent that the aspects of fraud prevention strategies were adopted by the bank

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deterrent security controls</td>
<td>4.021</td>
<td>0.892</td>
</tr>
<tr>
<td>Staff training and Development</td>
<td>4.469</td>
<td>1.063</td>
</tr>
<tr>
<td>Certification of auditors</td>
<td>3.917</td>
<td>0.794</td>
</tr>
<tr>
<td>Raising customer awareness about requirement to report changes</td>
<td>4.021</td>
<td>0.635</td>
</tr>
<tr>
<td>Peer review process</td>
<td>4.319</td>
<td>0.663</td>
</tr>
<tr>
<td>Following up on suspected frauds (Referring suspicious cases to the fraud teams)</td>
<td>2.072</td>
<td>1.121</td>
</tr>
<tr>
<td>Monitoring and evaluating various proactive initiatives</td>
<td>2.212</td>
<td>1.162</td>
</tr>
<tr>
<td>Evaluating defences and adjusting them in the light of experience.</td>
<td>2.861</td>
<td>1.125</td>
</tr>
<tr>
<td>Designing corporate fraud policies (Anti-fraud programmes)</td>
<td>2.229</td>
<td>0.953</td>
</tr>
<tr>
<td>Creating internal audit departments (Creation of anti-fraud culture / behaviours)</td>
<td>3.708</td>
<td>0.611</td>
</tr>
<tr>
<td>Implementing internal controls &amp; compliance</td>
<td>3.980</td>
<td>0.947</td>
</tr>
<tr>
<td>Whistle-blower systems</td>
<td>4.260</td>
<td>1.243</td>
</tr>
<tr>
<td>Publicizing fraud occurrences</td>
<td>3.820</td>
<td>1.041</td>
</tr>
<tr>
<td>Risk Identification &amp; Assessment (Identifying areas that are susceptible to abuse and make recommendations with regard to making systems more secure)</td>
<td>4.131</td>
<td>1.117</td>
</tr>
</tbody>
</table>
Adopting robust processes for verifying claims 3.837 0.275
Simplifying the claim process (system thinking in delivery of benefit service) 2.804 0.145
Ensuring staff involved in the administration of benefit are adequately trained and maintain the highest standard of probity – including completion of staff declaration 3.486 0.138
Pre-employment screening 2.901 0.471
Maintaining an accurate and complete asset register with clear asset descriptions 2.380 0.074
Carrying out regular stock-takes or spot-checks to confirm the existence of assets 2.720 0.347

The study sought to investigate whether the bank has a fraud policy in place. The interviewees indicated that there is a Group Fraud Policy that’s applicable to all Commercial banks in the world. The policy is maintained by the Group Financial Crime Risk CEO in UK.

Upon indicating that the bank has a fraud policy in place, the interviewees were required to highlight briefly the employed style /model of strategy implementation at bank. The study found that the group policy defines Fraud in its entirety and sets out the strategic direction, priorities and objectives for managing fraud risk. The policy sets out the blueprint for fraud control requirements, fraud risk assessments according to respective Business units and also lays out the general fraud control strategy providing fraud targets that units need to observe. The policy is structured into business units for ease of implementation and gives the escalation process.

The study further required the interviewees to comment on the bank’s fraud strategy with respect to the various aspects. With respect to authenticity of account opening documents, the interviewees indicated that opening of new accounts is the most robust process. The documents are verified at the point of entry (the branch or a Sales centre) by two designated bank officials. Verification is done through checking the copies against the originals. The documents are then forwarded to another department known as OPC for further processing. At this stage, the account opening documents are further checked. The bank also carries out a random check christened “the Eye-ball”. This is a random selection of account opening documents by a dedicated team of
Fraud Samplers. The team picks a sample at random and carries a thorough end to end authentication. When the process is satisfactory, the details of the applicant are forwarded to CRB for customer historical data. The entire process is lengthened because it’s considered to be the critical point of entry by customers into the banks network.

With regard to pre-employee screening, the interviewees said that this is an HR function. New employees have to be screened to ensure that only those candidates with clean records are taken on board. Applicants are required to submit certificates of good conduct obtained from the Director of CID. For those employees who have worked with other institutions within the banking industry, recommendations from their former employers are sought. The banks will also talk to the former employer directly to verify any information required. Otherwise all applicants for employment in Commercial have to submit at least three referees who must be reachable at short notice. The group code of conduct and Ethics sets out the standards to be embraced by all staff. It’s mandatory for new employees to the Bank to go through induction training on Fraud Management. They will also sign attestations that they have been trained and will strive in their employment to make the banks premises free from Fraud. The same is enforced by the Head of Security and Investigation (SIS). Fraud awareness is also a continuous exercise through refresher courses and also through Fraud Alerts.

On the transactions monitoring, the interviewees indicated that transactions in the bank are screened for normalcy and for anti money laundering (AML). The Bank’s IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be auctioned. The business sets out parameters to be used for monitoring and the parameters are reviewed consistently to be in tune with the Market. Transactions that are not in sync with customer operating range will be picked as red flags and will be looked into by relevant arms of the bank.

The interviewees also indicated that credit and debit card transactions are monitored by a team of Fraud Analysts who operate 24hrs. Their role is to check for any unusual transactions on customer’s accounts. For any irregularities, the customer is contacted to verify a transaction. When a customer declines a transaction, the Fraud Analyst will caution the card to avoid further
usage. An incident will also be raised at this stage for the matter to be investigated. This applies to usage of banking instruments such as cheques and transfer instructions (SWIFT, EFTs and RTGSs). Any abnormal usage or eye catching transactions detected on a customer’s account that are not in synch with a customer’s behavior, the bank will call the customer to verify the transactions. Some transactions that may fall on the AML radar are investigated and may be reported as suspicious transactions reports (STR’s) to CBK for further action under the prudential guidelines. Corporate and Premier Customers have fully dedicated relationship managers who keep an eye on their accounts on a regular basis and alert the customers for any suspicious transactions.

On the reporting processes of detected cases, it was found that the Head of Commercial Security and Investigations Services & Fraud Management (SIS & FM) is mandated to investigate all reported cases and make recommendations to the business executive committee on action to be taken. All business units within the country have 24hrs to report cases detected to the Head of SIS & FM. The business units will be required to raise an incident report and sent it to the attention of the Head of SIS & FM. For sensitive cases that use of normal escalation channels is believed to prejudicial, the bank has provided a whistle blowing facility. This will take care of cases that may involve officers of different ranks in the bank to avoid victimization. Whistle blow lines are maintained by the Head of SIS & FM and only him can retrieve information. The whistle blow facility allows a reportee / informer to make a report while remaining anonymous. Other than the internal channels, the Bank has also created a contact centre to receive complaints, reports and information from customers and disseminate the same to various relative centers for action. The Contact centre was set up in 2008 and is open 24hrs. The centre is mandated to also follow up the queries to the right departments to ensure that action has been done and appropriate communication has been provided to the customer. The department is based at the Banks main operations centre at Bishops Gate along Bishops road, in Nairobi

With regard to dispensations to open accounts, the interviewees indicated that there are no dispensations to open accounts. The bank operates a strict account opening policy and all customers have to meet the requirements to open accounts. The same is also monitored by
central Bank for compliance. As a measure of gravity of the process, Commercial Banks have created an independent unit to deal with account opening. The unit is known as KYC and main function is to receive account opening requests from Branches and verify them in detail for compliance with the group standards. They also liaise with other institutions of the Bank such as HR, SIS & FM and Compliance to make sure that customers taken on board into the Banks systems are good. KYC also works with other departments outside the Bank such as CRB, Principal Immigrations office and the principal registrar of persons to ensure that documentations provided to open accounts are valid.

The study also revealed that a whistle blowing facility is existent in the Bank. The facility sits with the Head of SIS &FM who downloads information from the receiving facility and allocates it for investigations. Reports that are sensitive an anonymity is desirable are reported through the facility. This is a very effective facility especially for checking high level internal frauds. The facility is free and available to all employees across ranks. Information is treated with utmost confidence and the whistle blowing line is displayed conspicuously on all Commercial centers for all to see and make good use.

With respect to online transactions (opening of new accounts, deposits, transfers, balance inquiries), the interviewees indicated that opening of accounts is an elaborate process which begins when a customer walks into a branch to open an account. The first encounter will be face to face where a Bank staff will receive customer documents and certify with the originals. The remaining process will be back office work and will not require the customer’s presence. Automation of the account opening process is not applicable in the Bank. Further, the Bank recently introduced a system known as “Hello Money” where customers can bank from the comfort of their rooms or offices. Customers can deposit money or inquire for balances in their accounts. To enlist into the facility, the customer needs to satisfy certain conditions which include good banking record in the bank. A customer enjoying the product must be able to keep secret codes such as PIN numbers off head to avoid compromise of card data. Customers under the category will sign indemnities to assure the bank that they will take due care of the bank codes and will solely use them for official use. To transact in the Hello money program,
customer will be issued with a secret PIN. The customer will be required to destroy the PIN after memorizing and henceforth apply the PIN on all the transactions. The Bank will verify the transactions when the customers PIN matches with the corresponding PIN in the Bank. This also applies to cash deposits on the ATMs.

The study further sought to identify the procedures in place to ensure that an employee doesn't award or manage a transaction where he or she has a financial interest in the vendor providing the product or services. The interviewees indicated that the bank operates on a “maker-checker” authorization process. A person posting a transaction will not authorize that transaction. It will be authorized by a person of a higher level for dual control. For tenders, the Bank has certain predetermined group of vendors who have been authorized to deal with the Bank. The vendors are selected after going through a due diligence process where their background is checked, their financial capability and integrity scales. The tendering committee will only recommend the choice of a vendor but will not make a final decision to award a tender. The final decision will rest with the Executive committee of the Bank chaired by the Chief Finance Officer (CFO). The segregation of function will make impossible for any interested person at any level to sway the process for his personal gain.

4.5 Fraud Related Risks Responses Improvement Strategies

The study sought to find out the respondents agreement level with statements that relate to fraud risks responses improvement strategies. A 5-point likert scale was used where 5-4.5= strongly agree; 4.995-3.5 = agree; 3.499-2.5 = neutral; 2.499-1.5 = disagree and 1.499-1.0 = strongly disagree.

According to the findings, the respondents strongly agreed that the bank has a fraud control plan documenting the responsibilities for fraud prevention, detection and response initiatives as shown by a mean of 4.667. in addition, the respondents agreed that the bank has a code of conduct clarifying the banks expectations for ethical behaviour that is demonstrably adhered to and promoted by senior management, employment and recruitment practices are scrutinized to ensure that only those new recruits to the business whose references have been taken up and
checked thoroughly are employed, there are periodic fraud risk assessments to identify and treat major fraud risks, and inform the fraud control plan and there is scrutiny by internal audit and the audit committee of the effectiveness of the bank fraud control framework and related activities and effective controls for activities with a high fraud risk exposure as shown by a mean of 4.457, 4.414, 4.414 and 4.367 respectively. Moreover, the respondents agreed that all major frauds occur because of poor internal controls or the overriding of these controls, systems and controls should be examined to identify weaknesses which make the company susceptible to the risk of fraud, there is a fraud policy establishing clear standards and procedures for dealing with suspected fraud incidents and there is regular staff fraud awareness training on their responsibilities for identifying, preventing and reporting potential wrongdoing as shown by a mean of 4.326, 4.174, 3.879 and 3.671 respectively.

Table 4. 7: Respondents’ agreement level with statements that relate to fraud risks responses improvement strategies

<table>
<thead>
<tr>
<th>Statement</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems and controls should be examined to identify weaknesses which</td>
<td>4.174</td>
<td>0.612</td>
</tr>
<tr>
<td>make the company susceptible to the risk of fraud.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employment and recruitment practices are scrutinized to ensure that only</td>
<td>4.414</td>
<td>0.923</td>
</tr>
<tr>
<td>those new recruits to the business whose references have been taken up and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>checked thoroughly are employed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The bank has a fraud control plan documenting the responsibilities for</td>
<td>4.667</td>
<td>0.802</td>
</tr>
<tr>
<td>fraud prevention, detection and response initiatives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There are periodic fraud risk assessments to identify and treat major</td>
<td>4.414</td>
<td>0.513</td>
</tr>
<tr>
<td>fraud risks, and inform the fraud control plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is a fraud policy establishing clear standards and procedures for</td>
<td>3.879</td>
<td>0.903</td>
</tr>
<tr>
<td>dealing with suspected fraud incidents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The bank has a code of conduct clarifying the banks expectations for</td>
<td>4.457</td>
<td>0.172</td>
</tr>
<tr>
<td>ethical behaviour that is demonstrably adhered to and promoted by senior</td>
<td></td>
<td></td>
</tr>
<tr>
<td>management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is regular staff fraud awareness training on their responsibilities</td>
<td>3.671</td>
<td>0.567</td>
</tr>
<tr>
<td>for identifying, preventing and reporting potential wrongdoing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is scrutiny by internal audit and the audit committee of the</td>
<td>4.367</td>
<td>0.592</td>
</tr>
<tr>
<td>effectiveness of the bank fraud control framework and related activities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
effective controls for activities with a high fraud risk exposure. All major frauds occur because of poor internal controls or the overriding of these controls.

The study sought to find out the extent respondents agree that the banks should adopt the strategies to ensure optimal response to the fraud risk. A 5-point likert scale was used where 5-4.5 = strongly agree; 4.99-3.5 = agree; 3.499-2.5 = neutral; 2.499-1.5 = disagree and 1.499-1.0 = strongly disagree.

From the findings the respondents strongly agreed that the banks systematically monitor and report on the effectiveness of their fraud control strategies, develop and maintain an up-to-date fraud control plan clearly documenting their fraud prevention, detection and response initiatives and responsibilities, establish arrangements that assure effective ongoing scrutiny by executive management, internal audit and audit committees, of the effectiveness of the fraud control framework and provide induction and periodic fraud awareness training to all council staff, to assure they understand their fraud control responsibilities as shown by a mean of 4.901, 4.872, 4.829 and 4.691 respectively. In addition, the respondents agreed that make sure accounts payable systems have effective preventative and/or compensating controls that adequately mitigate the risk of fraudulent purchases and/or payments and maintain accurate and an up-to-date asset registers that are regularly reviewed to mitigate the misuse and/or misappropriation of assets as shown by a mean of 4.208 and 4.108 respectively.

**Table 4. 8: Extent respondents agree that the banks should adopt the strategies to ensure optimal response to the fraud risk**

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop and maintain an up-to-date fraud control plan clearly documenting their fraud prevention, detection and response initiatives and responsibilities</td>
<td>4.872</td>
<td>0.211</td>
</tr>
<tr>
<td>Provide induction and periodic fraud awareness training to all council staff, to</td>
<td>4.691</td>
<td>0.603</td>
</tr>
</tbody>
</table>
assure they understand their fraud control responsibilities
Systematically monitor and report on the effectiveness of their fraud control strategies
Establish arrangements that assure effective ongoing scrutiny by executive management, internal audit and audit committees, of the effectiveness of the fraud control framework.
Make sure accounts payable systems have effective preventative and/or compensating controls that adequately mitigate the risk of fraudulent purchases and/or payments
Maintain accurate and an up-to-date asset registers that are regularly reviewed to mitigate the misuse and/or misappropriation of assets

On indicating that they believe that the Bank recognizes the role played by staff in the fight against fraud, the interviewees were required to state how they are recognized. Majority of the interviewees indicated that in line with the fraud culture, any staffs who manage to stop a fraud that would have culminated into a loss will receive mementos that range from certificates of recognition, gifts, promotions and even increased bonuses. This recognition will go into their files and one will be eligible to even promotions when opportunities arise. The Bank values good conduct and any demonstration of the same will be rewarded. Many types of awards such as the COO’s ward, the Chairman’s award are up for winning. The bank carries out on yearly basis an employee opinion survey (EOS) and the result has been favorable.

The study requested the interviewees to give recommendations on what could be done to reduce the incidences of Fraud in the Bank. The interviewees indicated that reforms in the police could help reduce the fraud related risks in the bank. They indicated that the police are charged with the responsibility of investigating and apprehending criminals. Frauds are perpetrated by criminals. It’s the work of the Police to carry out thorough investigations in order to punish criminals, penetrate into the underworld of fraudsters and frustrate their efforts. When police fall
back on this cardinal role or investigate poorly, Kenya can only become a destination of choice for fraudsters.

The interviewees also indicated that to reduce the fraud related risks in the bank there is need to relook at the judiciary. The interviewees argued that since the judiciary is a key player in Fraud Management and that over the time, it has been seen that courts often acquit or hand in lenient sentences to deadly fraudsters, the judiciary needs to be empowered through reform to be able to understand and be of help. The magistrates need to be exposed to international practices in developed countries where frauds have even driven banks to closure so that they understand the gravity of the problem. Those countries have now put in place strict laws to manage fraud; the result is that criminals in those countries are now running into countries like Kenya.

The interviewees also indicated that review of Fraud Legislation could reduce fraud related risks in the banks. Kenya still lags behind on anti fraud laws. The Anti-money laundering act was just passed the other day while others have not been passed. The Card industry in the country faces a real risk from fraudsters because supporting laws have not been enacted. The communications act and the rules of evidence in the country have to be reviewed to be in sync with the current challenges. Bank operations are now hi-tech on technology. The crimes have also spontaneously gone hi-tech therefore calling for amendments to the laws. For example, a person involved in ecommerce may engage in an electronic transaction with a client in Japan. The two partners will not meet face to face and there will be no binding executions to be made. When Fraud occurs, the Kenyan businessman will suffer. The situation will be worse if the instruction is hacked by a fraudster in between.

From the findings, it was also clear that review of security features of security documents (The Kenyan National ID, Driving licenses, passports and Title deeds) would also eliminate fraud related risks in the bank. The documents are main instruments that are recognized in the Banking industry in Kenya. The ID, Passport and Driving license is required to open accounts and to transact on the accounts; the title deed is collateral to obtain credit. The documents are now easily counterfeited and banks are exposed to greater risks. Kenya is becoming a destination of
criminals. The Nigerians, Bulgarians and Russians are flooding the market due to its ease in transit using fake documents. The documents are easily replicated in the streets and fraudulently used to access money in Banks. It’s possible to have 1000 ID cards in Kenya with different names. It’s even common for persons to circulate Fake currencies.

4.6 Chapter Summary

This chapter presents the findings of this study. The chapter covers general information, fraud detection, fraud prevention and fraud related risks. The next chapter presents the conclusion and recommendation of the study.
CHAPTER FIVE

5.0. DISCUSSION, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

This chapter provides the summary of the findings from chapter four, and also it gives the conclusions and recommendations of the study based on the objectives of the study. The objective of this study was to determine the responses by Commercial banks to fraud related risks in the banking industry.

5.2 Summary of the Study

The general objective of this study was to determine the responses by Commercial banks to fraud related risks in the banking industry. This was a case study since the unit of analysis was one organization aimed at getting detailed information regarding the strategic responses to increasing fraud risk at commercial banks. Primary data was collected using self-administered questioners. The questioners contained closed and open-ended questions. The open-ended questions enabled the researcher to collect qualitative data. Before processing the responses, the completed interview guides were edited for completeness and consistency. A quantitative analysis was employed. The quantitative analysis was used to analyze the questioners about the strategic responses to fraud risk in commercial

The study found that there are fraud detection strategies adopted by commercial banks in Kenya. Moreover, the banks employed estimating the extent of fraud and error within the system, using technology to gather data about symptoms, use of surveillance and tip-offs to a great extent. The banks employed use of covert operations and whistle-blowing to a moderate extent. There was no single test that a fraud has been committed.

The study found that there are fraud prevention strategies adopted by commercial banks. The banks adopted fraud prevention strategies to great extent. The respondents also indicated that
publicizing fraud occurrences and whistle-blower systems were adopted in the bank to a great extent.

There is a Group Fraud Policy that’s applicable to all Commercial banks in the world. The policy is maintained by the Group Financial Crime Risk CEO in UK. Upon indicating that the bank has a fraud policy in place, the interviewees were required to highlight briefly the employed style/model of strategy implementation at bank.

With respect to authenticity of account opening documents, the interviewees indicated that opening of new accounts is the most robust process. At this stage, the account opening documents are further checked. The bank also carries out a random check christened “the Eye-ball”. This is a random selection of account opening documents by a dedicated team of Fraud Samplers.

It was found that the Head of Commercial Security and Investigations & Fraud Management (SIS & FM) is mandated to investigate all reported cases and make recommendations to the business executive committee on action to be taken. Whistle blow lines are maintained by the Head of SIS & FM and only he can retrieve information. The study also revealed that a whistle blowing facility is existent in the Bank. The facility sits with the Head of SIS &FM who downloads information from the receiving facility and allocates it for investigations. This is a very effective facility especially for checking high level internal frauds. The facility is free and available to all employees across ranks. Information is treated with utmost confidence and the whistle blowing line is displayed conspicuously on all Commercial centers for all to see and make good use. The study found that the bank has a fraud control plan documenting the responsibilities for fraud prevention, detection and response initiatives.

5.3 Discussions

The study found that there are fraud detection strategies adopted by commercial banks in Kenya. Fraud detection strategies are adopted at the Commercial banks to a very great extent. This was in agreement with Sadgrove (2006) who suggested that for such a review to be carried out
successfully, one needs (a) to have adequate knowledge about both how fraud happens as well as about fraud indicators, and (b) to undertake a fraud vulnerability analysis of the company concerned. The banks employed specific investigation by management, forensic investigation, HR / disciplinary procedures and internal audit reporting & security to a great extent. In addition, the banks employed employee notification, use of informants and reviewing, analyzing the causes of fraud and error and fraud audit program to a great extent. Others Sorensen (1980) have proposed the use by auditors of the triangle model which comprises: (a) a strong, involved, investigative board of directors; (b) a sound, comprehensive system of internal controls; and (c) alert, capable independent auditors. Moreover, the banks employed estimating the extent of fraud and error within the system, using technology to gather data about symptoms, use of surveillance and tip-offs to a great extent. The banks also employed computer imaging and analysis and data mining tools, internal audit review, use of external sources of information, security / audit investigations and line management to a great extent. The banks employed use of covert operations and whistle-blowing to a moderate extent. There was no single test that a fraud has been committed. Most frauds involved an employee or manager of the victims' organization. The most effective tools for fraud detection are internal audit review, specific investigation by management, employee notification and accidental discovery. Whistle-blowing is considered as another way of detection. Whistle-blower is the employee who reports unethical and illegal practices in the place of work.

The interviewees indicated that fraud management in the bank is anchored on 5 key departments which include Compliance, Risk and Advisory services (RAS), Control and Governance (C&G), Internal Audit (IA) and Security and Investigations Services & Fraud Management (SIS & FM). All the departments work jointly as a team towards eradicating fraud. This was in agreement with Johnson et al.’s cognitive model, while management attempts to deceive the auditor by utilizing both their knowledge of the business and accounting practices as well as deep cognitive strategies and tactics (e.g. masking, double play, mimicking, dazzling, inventing, repackaging, decoying) and constructing a deception, auditors can use strategies and tactics (e.g anti-mimicking) for detecting such deceptions (Bernardi, 1994). The Compliance department deals with issues of account opening screening, due diligence on vendors and AML. They also
implement group sanctions. RAS is charged with carrying out risk tests on all new products that are to be introduced into the market. They carry out assessments on new and existing products to identify any loop holes that fraudsters can use to siphon money out. They ensure that sufficient controls are in place for new products to be rolled out. They also carry out continuous checks for existing products in the market to ensure that they updated in line with any changes in the operating environment. IA is the internal Audit function of the bank. Its role is to check whether requisite procedures are in place and are followed. Control & Governance department is a retail function that takes care of all control issues in the retail outlets (branches). The department is structured into regions headed by Senior Control Managers and their work is to ensure that control procedures are followed. SIS & FM is a Head office department. Its core function is advice on security matters, offer fraud training and carry out investigations. All cases are reported into the department for action. The department reports directly into the COO to insulate it from unnecessary influence. The team is charged with enforcing the Group Fraud Policy. Traditional statistical classification methods (Hand, 1981; McLachlan, 1992) such as linear discriminant analysis and logistic discrimination have proved to be effective tools for many applications, but more powerful tools (Webb, 2009), especially neural networks, have also been extensively applied.

The study found that there are fraud prevention strategies adopted by commercial banks. The banks adopted fraud prevention strategies to great extent. A weak internal control creates opportunities for fraud and about half of all frauds occur in the financial area (Vanasco, 2011). Certification of auditors, creating internal audit departments (creation of anti-fraud culture / behaviours) and implementing internal controls & compliance were adopted in the bank to a great extent. In addition, ensuring staff involved in the administration of benefit are adequately trained and maintain the highest, standard of probity – including completion of staff declaration, staff training and development, risk identification & assessment (identifying areas that are susceptible to abuse and make recommendations with regard to making systems more secure), deterrent security controls and adopting robust processes for verifying claims were adopted in the bank to a great extent. Internal control system has four broad objectives; those are to safeguard assets of the firm; to ensure the accuracy and reliability of accounting records and
information; to promote efficiency in the firm's operation; and to measure compliance with management's prescribed policies and procedures (Havey, 2009). Moreover, raising customer awareness about requirement to report changes, pre-employment screening, evaluating defences and adjusting them in the light of experience, simplifying the claim process (system thinking in delivery of benefit service) and maintaining an accurate and complete asset register with clear asset descriptions were adopted in the bank to a great extent. Katz, (2000) reveals diverse views regarding the classification of CAIS security controls. Security controls of CAIS could be classified according to their purpose: to deter; to prevent; to detect; and to correct security threats. The respondents indicated that peer review process, designing corporate fraud policies (anti-fraud programmes), monitoring and evaluating various proactive initiatives and following up on suspected frauds (Referring suspicious cases to the fraud teams) were adopted in the bank to a great extent. The respondents also indicated that publicizing fraud occurrences and whistle-blower systems were adopted in the bank to a great extent. Individual controls in each of the three categories, though being important, must complement each other. This necessitates an over-arching policy, which determines the nature of controls being implemented, and therefore provides a comprehensive security to the organization (Baker, 2009).

There is a Group Fraud Policy that’s applicable to all Commercial banks in the world. The policy is maintained by the Group Financial Crime Risk CEO in UK. Upon indicating that the bank has a fraud policy in place, the interviewees were required to highlight briefly the employed style /model of strategy implementation at bank. The study found that the group policy defines Fraud in its entirety and sets out the strategic direction, priorities and objectives for managing fraud risk. The policy sets out the blueprint for fraud control requirements, fraud risk assessments according to respective Business units and also lays out the general fraud control strategy providing fraud targets that units need to observe. The policy is structured into business units for ease of implementation and gives the escalation process.

With respect to authenticity of account opening documents, the interviewees indicated that opening of new accounts is the most robust process. The documents are verified at the point of entry (the branch or a Sales centre) by two designated bank officials. Verification is done
through checking the copies against the originals. The documents are then forwarded to another department known as OPC for further processing. At this stage, the account opening documents are further checked. The bank also carries out a random check christened “the Eye-ball”. This is a random selection of account opening documents by a dedicated team of Fraud Samplers. The team picks a sample at random and carries a thorough end to end authentication. When the process is satisfactory, the details of the applicant are forwarded to CRB for customer historical data. The entire process is lengthened because it’s considered to be the critical point of entry by customers into the banks network.

With regard to pre-employee screening, this is an HR function. New employees have to be screened to ensure that only those candidates with clean records are taken on board. Applicants are required to submit certificates of good conduct obtained from the Director of CID. For those employees who have worked with other institutions within the banking industry, recommendations from their former employers are sought. The banks will also talk to the former employer directly to verify any information required. Otherwise all applicants for employment in commercial banks have to submit at least three referees who must be reachable at short notice. The group code of conduct and Ethics sets out the standards to be embraced by all staff. It’s mandatory for new employees to the bank to go through induction training on Fraud Management. They will also sign attestations that they have been trained and will strive in their employment to make the banks premises free from Fraud. The same is enforced by the Head of Security and Investigation (BASIS). Fraud awareness is also a continuous exercise through refresher courses and also through Fraud Alerts. This was in agreement with Cressey (2007) who revealed that key preventative measures critical to a sound fraud control framework include: a fraud control plan documenting the responsibilities for fraud prevention, detection and response initiatives; periodic fraud risk assessments to identify and treat major fraud risks, and inform the fraud control plan; a fraud policy establishing clear standards and procedures for dealing with suspected fraud incidents; a code of conduct clarifying the council’s expectations for ethical behaviour that is demonstrably adhered to and promoted by senior management; regular staff fraud awareness training on their responsibilities for identifying, preventing and reporting potential wrongdoing; scrutiny by internal audit and the audit committee of the effectiveness of
the council’s fraud control framework and related activities; and effective controls for activities with a high fraud risk exposure

Transactions in the bank are screened for normalcy and for anti money laundering (AML). The Bank’s IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be auctioned. The business sets out parameters to be used for monitoring and the parameters are reviewed consistently to be in tune with the Market. Transactions that are not in sync with customer operating range will be picked as red flags and will be looked into by relevant arms of the bank. Porter (1993) indicated that red flags do not indicate the presence of fraud but represent conditions associated with fraud; in other words, they are cues meant to alert an auditor to the possibility of fraudulent activity.

Credit and debit card transactions are monitored by a team of Fraud Analysts who operate 24hrs. Their role is to check for any unusual transactions on customer’s accounts. For any irregularities, the customer is contacted to verify a transaction. When a customer declines a transaction, the Fraud Analyst will caution the card to avoid further usage. An incident will also be raised at this stage for the matter to be investigated. This applies to usage of banking instruments such as cheques and transfer instructions (SWIFT, EFTs and RTGSs). Any abnormal usage or eye catching transactions detected on a customer’s account that are not in synch with a customer’s behavior, the bank will call the customer to verify the transactions. Some transactions that may fall on the AML radar are investigated and may be reported as suspicious transactions reports (STR’s) to CBK for further action under the prudential guidelines. Corporate and Premier Customers have fully dedicated relationship managers who keep an eye on their accounts on a regular basis and alert the customers for any suspicious transactions.

It was found that the Head of Commercial Security and Investigations & Fraud Management (SIS & FM) is mandated to investigate all reported cases and make recommendations to the business executive committee on action to be taken. All business units within the country have 24hrs to report cases detected to the Head of SIS & FM. The business units will be required to raise an incident report and sent it to the attention of the Head of SIS & FM. For sensitive cases
that use of normal escalation channels is believed to prejudicial, the bank has provided a whistle blowing facility. This will take care of cases that may involve officers of different ranks in the bank to avoid victimization. Whistle blow lines are maintained by the Head of SIS & FM and only him can retrieve information. The whistle blow facility allows a reportee / informer to make a report while remaining anonymous. Other than the internal channels, the Bank has also created a contact centre to receive complaints, reports and information from customers and disseminate the same to various relative centers for action. The Contact centre was set up in 2008 and is open 24hrs. The centre is mandated to also follow up the queries to the right departments to ensure that action has been done and appropriate communication has been provided to the customer. The department is based at the Banks main operations centre at Bishops Gate along Bishops rd, in Nairobi

There are no dispensations to open accounts. The bank operates a strict account opening policy and all customers have to meet the requirements to open accounts. The same is also monitored by central Bank for compliance. As a measure of gravity of the process, Commercial Bank have created an independent unit to deal with account opening. The unit is known as KYC and main function is to receive account opening requests from Branches and verify them in detail for compliance with the group standards. They also liaise with other institutions of the Bank such as HR, SIS & FM and Compliance to make sure that customers taken on board into the Banks systems are good. KYC also works with other departments outside the Bank such as CRB, Principal Immigrations office and the principal registrar of persons to ensure that documentations provided to open accounts are valid.

The study also revealed that a whistle blowing facility is existent in the Bank. The facility sits with the Head of SIS &FM who downloads information from the receiving facility and allocates it for investigations. Reports that are sensitive an anonymity is desirable are reported through the facility. This is a very effective facility especially for checking high level internal frauds. The facility is free and available to all employees across ranks. Information is treated with utmost confidence and the whistle blowing line is displayed conspicuously on all Commercial centers for all to see and make good use.
Opening of accounts is an elaborate process which begins when a customer walks into a branch to open an account. The first encounter will be face to face where a Bank staff will receive customer documents and certify with the originals. The remaining process will be back office work and will not require the customer’s presence. Automation of the account opening process is not applicable in the Bank. Further, the Bank recently introduced a system known as “Hello Money” where customers can bank from the comfort of their rooms or offices. Customers can deposit money or inquire for balances in their accounts. To enlist into the facility, the customer needs to satisfy certain conditions which include good banking record in the bank. A customer enjoying the product must be able to keep secret codes such as PIN numbers off head to avoid compromise of card data. Customers under the category will sign indemnities to assure the bank that they will take due care of the bank codes and will solely use them for official use. To transact in the Hello money program, a customer will be issued with a secret PIN. The customer will be required to destroy the PIN after memorizing and henceforth apply the PIN on all the transactions. The Bank will verify the transactions when the customers PIN matches with the corresponding PIN in the Bank. This also applies to cash deposits on the ATMs.

The banks operate on a “maker-checker” authorization process. A person posting a transaction will not authorize that transaction. It will be authorized by a person of a higher level for dual control. For tenders, the Bank has certain predetermined group of vendors who have been authorized to deal with the Bank. The vendors are selected after going through a due diligence process where their background is checked, their financial capability and integrity scales. The tendering committee will only recommend the choice of a vendor but will not make a final decision to award a tender. The final decision will rest with the Executive committee of the Bank chaired by the Chief Finance Officer (CFO). The segregation of function will make impossible for any interested person at any level to sway the process for his personal gain.

The study found that the bank has a fraud control plan documenting the responsibilities for fraud prevention, detection and response initiatives as shown by a mean of 4.667. In addition, the respondents agreed that the bank has a code of conduct clarifying the banks expectations for ethical behaviour that is demonstrably adhered to and promoted by senior management,
employment and recruitment practices are scrutinized to ensure that only those new recruits to the business whose references have been taken up and checked thoroughly are employed, there are periodic fraud risk assessments to identify and treat major fraud risks, and inform the fraud control plan and there is scrutiny by internal audit and the audit committee of the effectiveness of the bank fraud control framework and related activities and effective controls for activities with a high fraud risk exposure. Moreover, the respondents agreed that all major frauds occur because of poor internal controls or the overriding of these controls, systems and controls should be examined to identify weaknesses which make the company susceptible to the risk of fraud, there is a fraud policy establishing clear standards and procedures for dealing with suspected fraud incidents and there is regular staff fraud awareness training on their responsibilities for identifying, preventing and reporting potential wrongdoing.

The respondents strongly agreed that the banks systematically monitor and report on the effectiveness of their fraud control strategies, develop and maintain an up-to-date fraud control plan clearly documenting their fraud prevention, detection and response initiatives and responsibilities, establish arrangements that assure effective ongoing scrutiny by executive management, internal audit and audit committees, of the effectiveness of the fraud control framework and provide induction and periodic fraud awareness training to all council staff, to assure they understand their fraud control responsibilities. In addition, the respondents agreed that make sure accounts payable systems have effective preventative and/or compensating controls that adequately mitigate the risk of fraudulent purchases and/or payments and maintain accurate and an up-to-date asset registers that are regularly reviewed to mitigate the misuse and/or misappropriation of assets.

The banks recognizes the role played by staff in the fight against fraud, the interviewees were required to state how they are recognized. In line with the fraud culture, any staffs who manage to stop a fraud that would have culminated into a loss will receive mementos that range from certificates of recognition, gifts, promotions and even increased bonuses. This recognition will go into their files and one will be eligible to even promotions when opportunities arise. The Bank values good conduct and any demonstration of the same will be rewarded. Many types of awards
such as the COO’s ward, the Chairman’s award are up for winning. The bank carries out on yearly basis an employee opinion survey (EOS) and the result has been favorable.

To reduce the fraud related risks in the bank there is need to relook at the judiciary. The interviewees argued that since the judiciary is a key player in Fraud Management and that over the time, it has been seen that courts often acquit or hand in lenient sentences to deadly fraudsters, the judiciary needs to be empowered through reform to be able to understand and be of help. The magistrates need to be exposed to international l practices in developed countries where frauds have even driven banks to closure so that they understand the gravity of the problem. Those countries have now put in place strict laws to manage fraud; the result is that criminals in those countries are now running into countries like Kenya.

Review of Fraud Legislation could reduce fraud related risks in the banks. Kenya still lags behind on anti fraud laws. The Anti-money laundering act was just passed the other day while others have not been passed. The Card industry in the country faces a real risk from fraudsters because supporting laws have not been enacted. The communications act and the rules of evidence in the country have to be reviewed to be in sync with the current challenges. Bank operations are now hi-tech on technology. The crimes have also spontaneously gone hi-tech therefore calling for amendments to the laws. For example, a person involved in ecommerce may engage in an electronic transaction with a client in Japan. The two partners will not meet face to face and there will be no binding executions to be made. When Fraud occurs, the Kenyan businessman will suffer. The situation will be worse if the instruction is hacked by a fraudster in between.

Review of security features of security documents (The Kenyan National ID, Driving licenses, passports and Title deeds) would also eliminate fraud related risks in the bank. The documents are main instruments that are recognized in the Banking industry in Kenya. The ID, Passport and Driving license is required to open accounts and to transact on the accounts; the title deed is collateral to obtain credit. The documents are now easily counterfeited and banks are exposed to greater risks. Kenya is becoming a destination of criminals. The Nigerians, Bulgarians and
Russians are flooding the market due to its ease in transit using fake documents. The documents are easily replicated in the streets and fraudulently used to access money in Banks. It’s possible to have 1000 ID cards in Kenya with different names. It’s even common for persons to circulate fake currencies.

5.4 Conclusions

The study concludes that fraud is very sensitive and that customers have immense fear of fraud and it impacts negatively on banks profitability where income lost through fraud would have been reinvested to foster growth. Higher profits for a business will indicate that a Bank management is having the right strategy thus sending a positive signal to the market.

The study also concludes that the worst fraud risk is identity theft where identification documents are easy to reproduce, fraudsters make parallel passports, IDs and driving licenses then use them to take over accounts. Technology has opened up operations in the banks to global connectivity; the banks are now branchless as all of them are wired together therefore a customer can go to any branch to carry out a transaction. This makes customer identification more difficult. Transaction processing times that was taking longer now take shorter times leaving little time for more keen checks. While technology increased turnaround times, it has also been used by fraudsters to commit frauds. Bank operations such as online transactions, swifts, transfers and other payments operate on technology platforms and customer data is also stored electronically. Information technology management is weak that exposes the bank to fraud in terms of access levels, audit trail and system changes. Other weak areas include internal frauds which involve collusion with fraudsters, plastics credit and debit card frauds and transactions which include forgery of cheques, forged instructions and consumer (Loan) frauds.

The study further concludes that cheque fraud is a common type of fraud mainly because customers with cheque books are not careful in ensuring that their books are kept in safe custody. Forgery is another common fraud which occurs where customer signatures on payments instruments such as cheques, cards, and transfer orders may be forged. It was also indicated that Card Fraud (Plastic) in BBK is also common type of fraud since BBK is an Issuing and
Acquiring bank. The Bank issues debit and credit cards to customers. It also acquires merchants who accept both local and International card payments by customers on its behalf. BBK processes payments on VISA, MasterCard and AMEX cards. Card Fraud is the most common area of Fraud in the Bank.

The study deduces that there is a Group Fraud Policy that is applicable to all Commercial banks in the world. The policy is maintained by the Group Financial Crime Risk CEO in UK which defines Fraud in its entirety and sets out the strategic direction, priorities and objectives for managing fraud risk. The policy sets out the blueprint for fraud control requirements, fraud risk assessments according to respective Business units and also lays out the general fraud control strategy providing fraud targets that units need to observe. The policy is structured into business units for ease of implementation and gives the escalation process.

With respect to authenticity of account opening documents, the study established that opening of new accounts is the most robust process. The documents are verified at the point of entry (the branch or a Sales centre) by two designated Bank officials. Verification is done through checking the copies against the originals. The documents are then forwarded to another department known as OPC for further processing. When the process is satisfactory, the details of the applicant are forwarded to CRB for customer historical data. The entire process is lengthened because it is considered to be the critical point of entry by customers into the Bank's network.

The study also reveals that transactions in the Bank are screened for normalcy and for anti-money laundering (AML). The Bank’s IT infrastructure is designed to support the monitoring process by producing daily reports and alerts to be actioned. The business sets out parameters to be used for monitoring and the parameters are reviewed consistently to be in tune with the Market. Transactions that are not in sync with customer operating range will be picked as red flags and will be looked into by relevant arms of the Bank. Further, it was clear that credit and debit card transactions are monitored by a team of Fraud Analysts who operate 24hrs, the Head of commercial banks Security and Investigations & Fraud Management (SIS & FM) is mandated
to investigate all reported cases and make recommendations to the business executive committee on action to be taken and that there are no dispensations to open accounts.

The study also revealed that a whistle blowing facility is existent in the Bank. The facility sits with the Head of SIS & FM who downloads information from the receiving facility and allocates it for investigations. Reports that are sensitive an anonymity is desirable are reported through the facility. Opening of accounts is an elaborate process which begins when a customer walks into a branch to open an account and the bank operates on a “maker-checker” authorization process.

5.5 Recommendations

5.5.1 Recommendations for Improvement

The study recommends that there should be reforms in the police. This could help reduce the fraud related risks in the bank. The police are charged with the responsibility of investigating and apprehending criminals. Frauds are perpetrated by criminals. It’s the work of the police to carry out thorough investigations in order to punish criminals, penetrate into the underworld of fraudsters and frustrate their efforts. When police fall back on this cardinal role or investigate poorly, Kenya can only become a destination of choice for fraudsters.

The recommends that since the judiciary is a key player in Fraud Management and that over the time, it has been seen that courts often acquit or hand in lenient sentences to deadly fraudsters, the judiciary needs to be empowered through reform to be able to understand and be of help. The magistrates need to be exposed to international practices in developed countries where frauds have even driven banks to closure so that they understand the gravity of the problem. The country should now put in place strict laws to manage fraud. This will reduce fraudsters in the country and hence ensure successful business on the banks in Kenya.

The study also recommends that review of Fraud Legislation could reduce fraud related risks in the banks. Kenya still lags behind on anti fraud laws. The Anti-money laundering act was just passed the other day while others have not been passed. The Card industry in the country faces a
real risk from fraudsters because supporting laws have not been enacted. The communications act and the rules of evidence in the country have to be reviewed to be in sync with the current challenges. Bank operations are now hi-tech on technology. The crimes have also spontaneously gone hi-tech therefore calling for amendments to the laws. The two partners will not meet face to face and there will be no binding executions to be made. When Fraud occurs, the Kenyan businessman will suffer. The situation will be worse if the instruction is hacked by a fraudster in between.

The study also recommends that review of security features of security documents (The Kenyan National ID, Driving licenses, passports and Title deeds) would also eliminate fraud related risks in the bank. The documents are main instruments that are recognized in the Banking industry in Kenya. The ID, Passport and Driving license is required to open accounts and to transact on the accounts; the title deed is collateral to obtain credit. The documents are now easily counterfeited and banks are exposed to greater risks. The documents are easily replicated in the streets and fraudulently used to access money in Banks. Therefore a reform of the security features would ensure reduction of fraud in the banking transactions.

Other recommendations suggested include staff Management where human beings need constant monitoring and motivation of staffs. Appropriate methods should be put in place deal with the situations. Methods such as employee screening, staff account monitoring, profiling of staff disciplinary cases, job rotation and enrichment are worth considering. Some functions of monitoring are better performed by immediate line Managers; others will be performed by HR. Areas such as access rights, audit trails and other upgrades on system capabilities are paramount and should be revisited to ensure the staff does not participate in fraud related transactions.

5.5.2 Recommendations for Further Studies

This study has explored the strategic responses by commercial banks to fraud related risks and established that fraud is very sensitive and impacts negatively on banks profitability. The overall effect of fraud can therefore not be ignored at any cost. There is therefore need to respond to these fraud related risks. This study has recommended adoption of various reforms in the bank
and in other arms of the government to reduce fraud related risks in the banks in Kenya. The study further recommends that another study needs to be done with an aim of investigating the effectiveness of the strategic responses to fraud related risks in the commercial banks in Kenya.
REFERENCES


Association of Certified Fraud Examiners (ACFE) (1996), Report to the Nation on Occupational Fraud and Abuse, ACFE, Austin, TX.


COSO (2004), Enterprise risk management – integrated framework, Committee of Sponsoring Organizations.


Rezaee, Z. (2004), Causes, consequences and deterrence of financial statement fraud, Critical Perspective on Accounting, in press.


Wells, J. (1997), Occupational Fraud and Abuse, Obsidian Publishing: Dexter, MI.


APPENDICES

Appendix I: Questionnaire

SECTION A: DEMOGRAPHIC INFORMATION

1. Gender: Male [ ] Female [ ]

2. Your age bracket (Tick whichever appropriate)
   18 – 24 Years [ ]
   25 - 30 Years [ ]
   31 - 34 years [ ]
   35 – 40 years [ ]
   41 – 44 years [ ]
   45 – 50 years [ ]
   Over 51 years [ ]

3. For how long have you served in the Bank?

<table>
<thead>
<tr>
<th>Duration</th>
<th>[ ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 2 years</td>
<td></td>
</tr>
<tr>
<td>2 – 5 years</td>
<td></td>
</tr>
<tr>
<td>6 – 10 years</td>
<td></td>
</tr>
<tr>
<td>11 years and more</td>
<td></td>
</tr>
</tbody>
</table>
4. What is your highest level of education?

<table>
<thead>
<tr>
<th>Certificate</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Diploma</td>
<td></td>
</tr>
<tr>
<td>Higher National Diploma</td>
<td></td>
</tr>
<tr>
<td>Bachelors</td>
<td></td>
</tr>
<tr>
<td>Masters</td>
<td></td>
</tr>
<tr>
<td>PhD</td>
<td></td>
</tr>
<tr>
<td>Professional qualification</td>
<td></td>
</tr>
<tr>
<td>(Specify)</td>
<td></td>
</tr>
</tbody>
</table>

SECTION B: MAIN ISSUES

FRAUD DETECTION

1. Are there fraud detection strategies adopted by First Community Bank in Kenya?
   Yes [ ] No [ ]

2. If yes, to what extent are the fraud detection strategies adopted at the Bank?
   Very great extent [ ] Great extent [ ]
   Moderate extent [ ] Little extent [ ]
   Not at all [ ]

3. To what extent do you employ the following fraud detection strategies in the Bank? Use a scale of 1-5 where 1= Very great extent and 5 = Not at all.

<table>
<thead>
<tr>
<th>Internal audit review</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific investigation by management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee notification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of Surveillance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of Informants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of external Sources of information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of Covert operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tip-offs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whistle-blowing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud Audit Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Imaging and Analysis and Data Mining Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security / Audit Investigations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forensic Investigation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR / Disciplinary Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Audit Reporting &amp; Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using technology to gather data about symptoms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewing and analyzing the causes of fraud and error</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estimating the extent of fraud and error within the system</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FRAUD PREVENTION**

4. Are there fraud prevention strategies adopted by bank?

Yes [ ]

No [ ]

5. If yes, to what extent are fraud prevention strategies adopted by the bank?

Very great extent [ ]

Great extent [ ]

Moderate extent [ ]

Little extent [ ]

Not at all [ ]
6. To what extent are the following aspects of fraud prevention strategies adopted by the bank?

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Very great extent</th>
<th>Great extent</th>
<th>Moderate extent</th>
<th>Little extent</th>
<th>Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deterrent security controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff training and Development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certification of auditors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Raising customer awareness about requirement to report changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer review process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Following up on suspected frauds (Referring suspicious cases to the fraud teams)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring and evaluating various proactive initiatives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluating defences and adjusting them in the light of experience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designing corporate fraud policies (Anti-fraud programmes)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creating internal audit departments (Creation of anti-fraud culture / behaviours)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementing internal controls &amp; compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whistle-blower systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Publicizing fraud occurrences</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Risk Identification & Assessment
(Identifying areas that are susceptible to abuse and make recommendations with regard to making systems more secure)

- Adopting robust processes for verifying claims
- Simplifying the claim process (system thinking in delivery of benefit service)
- Ensuring staff involved in the administration of benefit are adequately trained and maintain the highest standard of probity – including completion of staff declaration
- Pre-employment screening
- Maintaining an accurate and complete asset register with clear asset descriptions
- Carrying out regular stock-takes or spot-checks to confirm the existence of assets

<table>
<thead>
<tr>
<th>7. How effective are the various fraud control strategies adopted by the bank?</th>
</tr>
</thead>
<tbody>
<tr>
<td>…………………………………………………………………………………………………………</td>
</tr>
<tr>
<td>………………………………………………………………………………………………………………..</td>
</tr>
<tr>
<td>………………………………………………………………………………………………………………..</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. How can the fraud management strategies adopted by the bank be enhanced?</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………………………………………………………………………………………………..</td>
</tr>
<tr>
<td>………………………………………………………………………………………………………………..</td>
</tr>
<tr>
<td>………………………………………………………………………………………………………………..</td>
</tr>
</tbody>
</table>