

MAKERERE UNIVERSITY
COLLEGE OF BUSINESS AND MANAGEMENT SCIENCES

TOPIC

**THE ROLE OF OPERATIONAL RISK MANAGEMENT STRATEGIES IN
COMBATING FRAUD IN FINANCIAL INSTITUTIONS.**

CASE STUDY

STANDARD CHARTERED BANK

BY

NAME: ROSETTE NAMANDA

REGISTRATION NUMBER: 2009/HD06/15396U

STUDENT NUMBER: 209019280

SUPERVISOR: MR. ABIBI FRANCIS

**A research report submitted to Makerere University in partial fulfilment for the award of
Masters' Degree in Business Administration**

DECLARATION

I, Rosette Namanda, declare that this is my own work, and it has never been presented for an Award of any University.

Researcher

Signature

Date.....

Rosette Namanda

Supervisor

Signature

Date.....

Mr Abibi Francis

DEDICATION

To all my family members, my supervisor Mr.Abibi Francis who has been so kind and helpful and to all my colleagues at Standard Chartered Bank

LIST OF ACRONYMS

SCB:	Standard Chartered Bank
CIMA:	Chartered Institute of Management Accountants
UBA:	Uganda Bankers Association
BOU:	Bank of Uganda
USA:	United States of America
UK:	United Kingdom
UCB:	Uganda Commercial Bank
STR:	Suspicious Transaction Reporting
CBS:	Basel Committee on Banking Supervision
ORM:	Operational Risk Management

TABLE OF CONTENTS

DECLARATION	ii
DEDICATION & APPROVAL	iii
LIST OF ACRONYMS	iv
LIST OF TABLES	vii
LIST OF FIGURES	viii
ABSTRACT	ix
CHAPTER ONE	1
1.0 INTRODUCTION	1
1.1 BACKGROUND TO THE STUDY	1
1.2 RISK	3
1.3 FRAUD	5
1.4. STATEMENT OF THE PROBLEM	7
1.5 THE OBJECTIVES OF THE STUDY	8
1.6 SCOPE OF THE STUDY	9
1.7 SIGNIFICANCE OF THE STUDY	9
CHAPTER TWO	10
2.0 LITERATURE REVIEW	10
2.1 OPERATIONAL RISK MANAGEMENT	10
2.2 OPERATIONAL RISK-THE REGULATORY FRAME WORK	11
2.3 FRAUD	15
2.4 THE RELATIONSHIP BETWEEN OPERATIONAL RISK MANAGEMENT AND COMBATING OF FRAUD IN FINANCIAL INSTITUTIONS	21
CHAPTER THREE	23
3.0 METHODOLOGY	23
3.1 RESEARCH DESIGN	23
3.2 AREA AND POPULATION OF STUDY	23
3.3 SAMPLE SIZE AND SAMPLING TECHNIQUE	23
3.4 SOURCES OF DATA COLLECTION	25
3.5 VARIABLES UNDER STUDY	25
3.6 DATA MANAGEMENT AND ANALYSIS	26
3.7 PROCEDURE OF THE STUDY	26
3.8 LIMITATIONS OF THE STUDY	26

CHAPTER FOUR	27
4.0 DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS	27
4.1 DEMOGRAPHIC CHARACTERISTICS	27
4.2 INFERENCE STATISTICS	30
CHAPTER FIVE	38
5.0 SUMMARY, CONCLUSION AND RECOMMENDATIONS	38
5.1 SUMMARY AND CONCLUSION	38
5.2 RECOMMENDATIONS	39
REFERENCES	43
APPENDIX A	45

LIST OF TABLES

Table 3.1: Distribution of respondents per department	24
Table 4.1: The impact of operational risk management in combating fraud	31
Table 4.2: Level of risk management and fraud	33
Table 4.3: The effectiveness of operational risk management in combating fraud	34
Table 4.4: Creative measures of operational risk management in combating fraud	35

LIST OF FIGURES

Figure 2.1: The fraud triangle	18
Figure 4.1: Percentage distribution of respondents by sex	27
Figure 4.2: Percentage distribution of respondents per role	28
Figure 4.3: Percentage distribution of respondents per department	29
Figure 4.4: Percentage distribution of respondents by number of years in the Departments	30

ABSTRACT

The study aimed at establishing the role of operational risk management in combating fraud in banking institutions focussing on Standard Chartered Bank Ltd. The specific objectives that guided the study were: to assess the impact of operational risk management in combating fraud, to establish the relationship between operational risk management and fraud, to explore creative measures of operational risk management in combating fraud to acceptable level and to assess the effectiveness of operational risk management in combating fraud.

Operational risk is not new. However significant operational risk events in the recent years have high lightened the need to manage operational risk more effectively. Banks should take a broader and a more holistic approach to operational risk management. Operational risk must be managed throughout the whole organisation in order to minimise losses resulting from frauds

Effective operational risk analysis is an integral process covering analysis of causes and events. Analysis should be designed to assist greater understanding of risks and improve management's ability control risks and allocate resources appropriately

Banking operations are further monitored by Bank of Uganda which is mandated by the financial institutions act 1993 to intervene in the activities of all banking institutions in order to minimise risks of fraud, insolvency, unsatisfactory corporate governance and gross mismanagement.

A cross sectional research design was used to collect data from various departments at Standard d bank such as Operations, Credit, risk/ Audit and Treasury departments.

Purposive sampling technique was used to select 50 respondents from the staff of Standard Chartered bank. Information on each of the variables was examined using the analytical research design.

Data was analysed by using S.P.S.S (Statistical Package for social scientists. The findings of the study are represented in graphs and pie charts. The decisions were made basing on highest percentages and frequencies from primary data gathered to establish the role operational risk management strategies in combating fraud in financial institutions, more especially Standard Chartered Bank.

Findings revealed that operational risk management strategies greatly impact on the risk of fraud, hence the risk of fraud reduces greatly as operational risk management measures are strengthened

Findings from the study revealed that fraud is still persistent in banking institutions as a result of system failures, failure to implement operational risk management programs, lack of motivation among the members of staff, lack of training and awareness programs, low levels of ethics and

integrity among members of staff, lack of technological advancements and failure incorporate all staff at levels while designing policies and coming up with operational risk management strategies.

In their drive to combat the risk of fraud, banking institutions should put emphasis on departments that are directly involved in operational risk activities. This could be done through regular trainings and awareness programs to equip the staff members concerned with the necessary skills for successful mitigation of the risk of fraud. The staff in the various departments should be motivated to encourage them to minimise fraud by being vigilant while attending to customers, reporting any suspicious transactions, emphasising best practises, sharing personal experiences

It is therefore very important for banking institutions to come up with strategies to address operational risk management measures to combat the risk of fraud. Banking institutions should also endeavour to review all strategies in place periodically.

CHAPTER ONE

1.0 INTRODUCTION

1.1 BACKGROUND TO THE STUDY

Risk management is an increasingly important process in many businesses. Business risks are proliferating in an increasingly competitive world today and this is beyond dispute. Risks to business continuity and to intangible assets such as intellectual property and reputation are rising as the economy becomes ever more global.

According to CIMA, Fraud and Risk Management (2007 and 2008) risk management process fits well with the precepts of good governance

Globally there has been a series of high profile corporate fraud and accounting scandals in various companies such as Barings Bank in Tokyo, Enron and WorldCom in the USA, Maxwell and Polly Peck in the UK, Green land Bank, International Credit Bank and Co-operative Bank in Uganda to mention but a few. The failure of most of these companies were characterised by misusing or misdirecting of funds, understating expenses, overstating revenues, under reporting the existence of liabilities and this was possible in co-ordination with officials in their affiliates.

Risk Management lies at the heart of all financial institutions such as insurance, banking and investment. Effective risk management is a central part of financial and operational management of financial institutions and is fundamental to the ability of financial institutions to generate profits consistently and maximise the interests of shareholders and other stakeholders.

Standard Chartered Bank is a foreign Bank with its headquarters in the UK. As one of the authorised operating commercial banks in Uganda, Standard Chartered bank Uganda limited was licensed to carry out business in Uganda in 1912 and has an estimated market share of 20%. It is the second largest bank in the market in terms of balance sheet size and profitability. The bank has 11 branches within the country spread across the following major towns; Kampala (7), Jinja (1), Mbarara (1), Mbale (1) and Gulu (1) and employs a total of 599 employs.

The strategic intent of Standard chartered Bank Uganda Limited is to lead the way in the banking industry in Uganda by being the Bank of choice for their chosen customer segments. In addition to the strategic intent, the bank has core values and these include; Responsive, Trustworthy, Creative, International and Courageous

Standard chartered bank as a commercial bank, offers a range of retail and wholesale banking products and services designed to exceed their customers' expectations, such products as current accounts, savings accounts, foreign exchange services, safe custody, fixed deposit accounts, credit facilities, discounting of bills and many others and they are the market leaders in product and service innovation.

In addition to their core banking business, they are committed to driving a strong sustainability agenda by making a positive contribution to the communities in which they operate through their community partnership initiatives such as "Seeing is Believing" where they partner with sight savers to restore sight to blind people and "Nets for Life" where they distribute insecticide treated bed nets to prevent the spread of malaria.

The bank's strategic intent is to lead the way in the banking industry in Uganda by being the banker of choice for their chosen customer segments.

In the need to exceed their customers' expectations, Standard Chartered Bank employs a team of well trained and experience employees but as they strive to offer excellent services to their customers, there are a lot of risks associated with their services and the bank has to make sure that these risks are managed adequately.

In the bid to ensure quality service and meeting customers' expectations, Standard Chartered Bank and other banks inclusive face a lot of risks and they should ensure that these risks are adequately managed

In 1998 Uganda's banking sector was in crisis, some banks were closed and for some, Bank of Uganda took over their management (African Business 1999)

Uganda's banking sector began to tremble tremendously in October 1998 when Trust Bank Uganda a subsidiary of Trust bank of Kenya experienced a run on its deposits when its parent bank was forced into closure. More banks such as International credit bank and Trans African Bank were also closed.

The biggest blow that the banking sector experienced was in December 1998 when Uganda's largest commercial bank (UCB) was purchased through Greenland Bank.

In Standard Chartered Bank, risk management lies at the heart of the bank's business. Effective risk management is a central part of the bank's financial management and fundamental to the bank's ability to generate profits consistently and maximise the interests of shareholders and other stakeholders. Risk management is a bank- wide activity and it begins at the frontline. The bank's strategic intent when it comes to risk management is to become the world's best risk function-leading the way in upholding the integrity of the bank's risk and return decision

1.2 Risk

Risks are potential events that could influence the attainment of an organisation's objectives. Risks should be managed to minimise losses, impact and frequency of failures and the likelihood of reputational damage

Management of risks entails understanding the nature of such events and where they represent threats, and thus making positive plans to combat them.

Management of risks is therefore increasingly an important process in banking institutions, and the process fits in well in the precepts of good corporate governance.

Management of risks should be a proactive, anticipative, and a reactive process that continuously monitors and controls risk.

According to Chance 2003, Management of risks is the process of identifying the level of risk that an entity desires, measuring the level of risk that an entity currently has, taking actions that bring the actual level of risk to the desired level of risk, and monitoring the new actual level of risk so that it continues to be aligned with the desired level of risk. The process is continuous and may require alterations in any of these activities to reflect new policies, preferences and information.

Risk management techniques employed by banks should not be retrospective; they should be designed to manage future risks in the vicious cycle of risks. In principle, management of risks is an area that involves looking ahead for things that might happen, and taking action in advance (Leitch 2003). Banks should learn from their past experiences and be able to forecast future risks and risk information needs to be interpreted dynamically

1.2.1 Types of Risks

In the financial industry, risk arises from many different activities such as investments, loans, sales, purchases, legal transactions, economic downturn, internal processes/systems failure, negative publicity, etc. In general the management of risks in financial sector (banks) risks are categorised into the following inter-related areas

- Regulatory risks
- Systematic risk
- Financial risk
- Strategic and Business risk
- Operational risk
- Credit risk
- Liquidity risk
- Market risk

Regulatory risks: regulatory developments and their impact on financial institutions

Systematic risk: risks of systematic crisis to the financial system as a whole triggered by financial institutions, and/or the risks to the financial service industry of such a systematic crisis, however triggered.

Financial risks relate to financial performance like profitability. These result into a loss for a bank if they are not properly managed. Financial risks are also subject to the complex interdependencies that may significantly increase a bank's overall risk profile. For example a bank engaged in foreign currency, business is normally exposed to currency risk

Credit risk occurs when dealing with customers, vendors, and other counterparties. It is generally viewed as the risk of default on an obligation. The BCBS defines credit risk as a risk which "occurs whenever a firm is exposed to loss if another party fails to perform its obligations".

Market risk arises from exposure to fluctuations in market prices, including exchange rates, commodity prices, and interest rates. According to the Basel Committee on Banking Supervision (BCBS), market risk is "the risk that arises from fluctuations in the values of, or income from, assets". In other words, it is the possibility of loss on investments or trading operations due to changes in the market.

Strategic and Business risks are associated with the bank's business environment, including macroeconomic and policy concerns, legal and regulatory factors and the overall financial sector infrastructure and payment system. Other forms of Business risk may be legal liability, Regulatory compliance, and reputational and fiduciary, country risk.

Events risks include all types of exogenous risks which, if they were to materialise, could jeopardize a bank's operations or undermine its financial condition and capital adequacy. Events risks may come as a result of political, Banking crisis and other exogenous factors.

Operational risks are associated with human error, system failures, and insufficient procedures and controls. The BCBS defines it as "the risk of loss, resulting from inadequate or failed internal processes, people, or systems, or from external events". Compliance with bank policies and procedures and measures against mismanagement and fraud. The operational risks may also involve; internal fraud, External fraud, Damage to physical assets, Business disruption and system Failures, employment practises and workplace safety etc.

The changing environment in which banks find themselves present a major opportunity for the banks, but also entails complex, variable risks that challenge traditional approaches to bank management. Banks must therefore quickly gain operational risk management capabilities in order to survive in a market oriented environment, in order to withstand competition from foreign banks and support private sector led economic growth.

The banks' awareness of operational risk and efforts to manage these risks has improved with the desire to enhance operating efficiency, reduce earnings volatility and rationalise capital allocation between strategic business units.

However many banks however are largely unclear about the benefits, to the business unit of investment in operational risk management tools.

Various lessons have been learnt from the recent Operation risk failures, such as the collapse of the Barings, Britain's oldest merchant Bank (200 years), One mark lee son, in Singapore managed to circumvent internal systems and hide his losses for an extended period of time, and thus over \$1.2 billion dollars was lost due to poor internal controls and failure of technology to detect trading and booking anomalies (Kigenyi 2006)

In the Banking sector today, both local and foreign, there is a great variation in attitude towards the operational risk management, as some banks are;

- Fearful institutions that do not want to be vulnerable to operational risk failures just like the case of Barings or One marl lees on Banks.
- Some banks are regulatory driven, and thus they carry out risk management because it's a requirement by the regulators.
- Some Banks are on a positive note visionary, and thus they understand the importance of operational risk management to their business and to their customers.

Fraud risk is one component of operational risk that is associated with events in transaction processing or other business operations. Fraud risk review therefore considers whether theses errors or events could be a result of deliberate act designed to benefit the perpetrator Fraud risks need to be assessed for each area and process of the business, for example cash payments, cash receipts, purchasing expenses, inventory, payroll, fixed assets and loans(CIMA, fraud risk management (2007).2008).

Liquidity Risk. Liquidity refers to the ability of company to make payments as they become due. Financial institutions that are solvent can and sometimes do fail because of liquidity problems

1.3. Fraud

Fraud can be defined as any form of behaviour by which one intends to gain a dishonest advantage over another, and it is thus an act or omission intended to cause wrongful gain to one person and wrongful loss to the other either by way of concealment of facts or otherwise.

Fraud essentially involves using deception to dishonestly make a personal gain for oneself or create a loss for another. (Fraud Act 2006)

According to Naita 2005, the areas of fraud may include; illegal/irregular manipulation of records and documents, forgery of documents such as vouchers, records, falsification of financial documents, unauthorised credit facilities extended for consideration, forgery in demand drafts, issuance of fake drafts and false letters of credit submission.

In banks people commit frauds due to the following (CIMA, fraud risk management (2007).2008); motivation of potential offenders, conditions under which people can rationalize their prospective crimes away, opportunities to commit fraud, technical ability of the fraudster, expected and actual risk recovery after the fraud has been carried out

Fraudsters usually fall into one of the 3 categories below

- Pre-planned fraudsters, who start out from the beginning intending to commit fraud
- Intermediate fraudsters, who start off honest but turn fraud when times get hard or when life events such as irritation at being passed over for promotion change the normal mode
- And slippery-slope fraudsters who simply carry on trading even when objectively they are not in position to pay their debts. This can only apply to ordinary traders or to major business people.

We realise that banks and financial institutions worldwide today are undergoing a sea change and face an environment marked by growing consolidation, rising customers' expectations, increasing regulatory requirements, proliferating engineering, uprising technological innovation and mounting competition. This has increased the probability of failures or mistakes from operations point of view.

It would be a mistake to conclude that the only way to succeed in banking is through ever greater size and diversity, indeed better risk management may be the only truly necessary element of success in banking.

Operational risk losses have often led to the downfall of financial institutions with more than 100 reported losses exceeding US\$100 million in the recent years (American Bankers Association Annual report, 2004). In the attempt to curb operational losses and formulate healthier banking environment, compliance bodies such as Basel II, mandate a focus on operational risk, forcing financial institutions to identify, measure, evaluate, control and manage the ubiquitous risk.

In Uganda the central Bank (BOU) has also emphasised numerous operational risk management measures in order to curb losses in banks such as KYC (Know your customer) aimed at knowing the customers better KYE (Know your employee) aimed at knowing the skill and competence of staff, AML (Anti money Laundering) policies, Suspicious transaction monitoring and reporting (STR) and call backs before payments are done. All these are aimed at curbing fraudulent activities in commercial banks.

In Standard Chartered Bank risk lies at the heart of the bank's business. Effective risk management is a central part of the bank's financial management and fundamental to their ability to generate profits consistently and maximise the interests of shareholders and stake holders, it is the bank's wide activity and begins at the frontline. Despite all the efforts, the bank continues to lose money due to failed operations. There are cases where tellers deposit money on wrong customer accounts and this money is never recovered. Paying customers excess money is very common among many branches of the bank, A customer one day walked into the bulk section of the bank at one of the branches with a cheque amounting to five million shillings, the teller at the counter carried out the correct posting of the cheque but at the time payment, an error occurred, fifty million shillings was paid to the customer instead of five million shillings, although the Bank security system (CCTV cameras) were up and running the bank tried to recover the money but failed.

Other forms of fraud reported included;

A customer walked into one of the Standard Chartered branches, and hardly an hour into the banking hall, he started claiming that he had lost five thousand United States Dollars to some unscrupulous person within the bank at that time. The Bank security system (CCTV cameras) was under preventive maintenance at that moment and no images could be retrieved to give justification of what had taken place. Customer however made attempts to recover the money lost from the bank, and all attempts failed.

A customer entrusted his agent to make subsequent deposits into his Standard Chartered bank account. The agent never made the deposits to the customer's account, but instead he obtained a forged stamp that he used to stamp the deposit counterfoils to provide justification that subsequent deposits had been made to the customer's account. When the customer obtained his account statement from the bank, none of the deposits was reflected on to his account, and it was thus discovered that stamps on the deposit counterfoil slips given to the customer by his agent had been forged.

1.4 STATEMENT OF THE PROBLEM

Despite all the operational risk management interventions, fraudulent activities have become persistent with in the Commercial Banks, more especially Standard Chartered Bank as highlighted above

This situation however if left unchecked will seriously affect the ability of the Banking Institutions to extend financial services to the targeted population groups, cause losses to the Banks and tarnish the reputation of the Banking system in the long run.

The researcher therefore carried out a study to find out whether there is a relationship between operational risk management and fraud in banking institutions.

1.5 THE OBJECTIVES OF THE STUDY

These set out what the study hoped to achieve.

1.5.1. General Objective

To establish the role played by operational risk management strategies in combating frauds in financial institutions such as banks

1.5.2. Specific objectives

To determine the impact of operational risk management in combating fraud in Standard Chartered Bank

To ascertain the relationship between Operational risk management and Fraud.

To determine the effectiveness of operational risk management in combating fraud in Standard Chartered Bank

To explore more creative techniques of operational risk management to combat fraud to an acceptable level.

1.5.3. Research Questions

What is the impact of operational risk management in combating fraud in Standard Chartered Bank?

What relationship is there between Operational risk management and Fraud in Standard Chartered Bank?

To what degree has Operational risk management reduced the risk of fraud in Standard Chartered Bank?

What creative techniques can operational risk management employ to combat fraud to an acceptable level in standard Chartered Bank?

1.6. SCOPE OF THE STUDY

The study focused on the operations of Standard Chartered bank for the period 2008 to 2013 targeting the operations department specifically. Standard Chartered bank was selected for this study because it's a commercial bank with a well-established operations department. Standard Chartered bank is represented in most of the major towns in Uganda and has a large customer base.

The study included employees of standard Chartered bank in the operations department, and employees in the management positions and these are the heads of departments and section heads situated at the head office of Standard Chartered

1.7. SIGNIFICANCE OF THE STUDY

They study was mainly meant for the partial fulfilment of the requirement for the award of a master's degree in Business Administration.

When the study is concluded, it will add more knowledge in the area of operational risk management.

The results of the study will be used by management of Standard Chartered Bank to improve on ways of managing operational risks.

The study will be of great importance to other financial institutions especially banks as it may expose loopholes in risk management strategies employed by banks, hence it may be a point of reference for banks to improve on their risk management techniques.

The recommendations that were made after the study may be used to stimulate policy debate among various stakeholders of the Banking institutions at both local and national levels, in a bid to create a healthier Banking environment.

The study will be of great importance to other researchers willing to explore the same field or other related topics.

CHAPTRE TWO

2.0 LITERATURE REVIEW

Under this section, the researcher viewed literature related to the study under investigation. The literature was obtained from various sources. The literature comprises of literature on operational risk management, fraud and the relationship between operational risk management and combating of fraud in banking institutions

2.1 OPERATIONAL RISK MANAGEMENT

2.1.1 Theoretical Review

According to CIMA, Fraud Risk management (2007) defines operational risk management as a continual cyclic process which includes risk assessment, risk decision making, and implementation of risk controls, which result in acceptance, mitigation, or avoidance of risk.

Operational risk management is the oversight of operational risk, and it includes risk of loss resulting from inadequate or failed internal processes and systems, human factors or from failed events.

The term operational risk is a recent phenomenon in the context of Banking and financial institutions, worldwide financial institutions began to recognise operational risk in the 1990s according to the Global Journal of finance and Banking issues Vol.2.No.2.2008.

Interest in regulation of operational risk was picked since the late 1990s after a number of high profile incidents and losses (Barings and others) and this gave rise to the treatment of operational risk under the Basel Accord (2004). Also the Basel committee's interest in making the New Basel Capital Accord more risk sensitive and the realisation that risks other than credit and market could be substantial, led to the explicit recognition of operational risk in the capital adequacy framework.

According to Basel Committee (2004), Operational risk is defined as the risk of loss resulting from inadequate or failed internal control processes, people and systems or from external events. The definition however includes legal risk, but excludes strategic and reputational risk. Operational risk may materialise directly as in the case of say, wire transfer (transfer of funds to the wrong person) or could indirectly as a credit or market loss.

Imad A. Moosa (2007) argues that the factor between pure market and credit losses and those linked to operational risk must be the cause. Moose (2007) argued that distinction should be made between the cause and the factor driving severity, stating that the cause of the Barings disaster was an operational loss, and thus given the close linkage of operational risk with

other types of risk, it's very important for Banks to have a clear understanding of the concept of operational risk before designing the operational risk measurement and management framework.

According to Halim Alamsyah, Jakarta, Indonesia 2008, Asian Banks that have suffered huge losses in the past, today make more serious look at insurance as an integral part of their operational risk management strategy, and thus Indonesian Banks may incur significant losses if they do not focus on operational risk management. Operational risk management should be limited to those that arise as a result of interaction between human beings and systems. To them doing credit business is not part of operation risk, yet there are those who think that human interactions in the business, institutional systems and doing credit as a business are part of operational risks.

Thus there is a need for greater emphasis to Banking institutions to adopt both the preventive and corrective aspects of operational risk control and develop policies and procedures that form the core of the organisation's internal control system. These operational guidelines should be reviewed and revised periodically in order to reduce vulnerabilities to operational risks.

2.2. Operational risk- The regulatory frame work

2.2.1. Basel committee guideline

The committee and the EU commission presented in 2001, a proposal for new capital adequacy rules. The rules were intended to replace original rules on capital adequacy requirements for credit risk set up in 1980; this was the major Basel 1 committee requirements, 1988 (Opiokello, 2006)

The objectives of the new regulation are to; promote safety and soundness of the financial system, enhance competitive equality, constitute a more comprehensive approach to addressing risk and provide capital adequacy approaches that are sensitive to the degree of risk by position and activity.

In respect to operational risk, Basel II provides that management of specific operational risk is not a new practise, and thus it has always been important for banks to try and prevent fraud, maintain integrity of internal controls and reduce errors in transaction processing etc.

2.2.2. Central Bank guide lines

Each of the East African Central Banks has issued Risk management guidelines in their own countries that include;

Bank of Uganda-Risk management guidelines, 2005;

Bank of Tanzania and Bank of Kenya-Nov 2003

Among others, the East African Bank regulators recognise the need for the following:

Board and management oversight, policies, processes and procedures, identification and measurement, Monitoring and control mechanisms.

In the classification of various types of risk, Operational risk generally includes all other risks except Credit and Market risk, and this type of risk is mainly associated with and arises from banking transactions.

Due to the potential losses that can result from the various banking transactions, and the need to observe the appropriate guidelines to manage exposure in such transactions, there is a great need for operational risk management to be taken seriously by bank management, regulators and investors (Kigenyi 2006).

Banks awareness of operational risk and efforts to manage it has to a limited extent improved with the desire to enhance operating efficiency, reduce earnings volatility and rationalise capital allocation between strategic business units. Many Banks are however unclear about the benefits for the business units, from the investment in operational risk management tools.

In the Banking industry, it has been greatly observed that failure to observe proper risk management in form of undertaking sufficient public disclosure to assist market participants assess the bank's operational risk exposure, assessment of processes for operational risks, emphasis on internal controls and mitigating policies and procedures, Board of Directors and senior management to set up and review operation risk framework and strategy, the Banks become vulnerable to fraud, which may have devastating effects on the Bank reputation, Customers, the unsuspecting public, together with other stakeholders.

2.2.3. Management of operational risk

It has become more than a recognised fact over the last decade that large bank losses originated from vulnerabilities in the operational processes and threats which together cause operational loss events. One striking example is the collapse of Barings Bank in 1996 where misuses of accounts (“assets”) by a rogue trader (“threat”), lack of accounting controls and audit as well as inappropriate segregation of duties (“vulnerabilities”) were at the source of fraudulent transactions. As can be seen in this example, although IT risk has to be considered and constitutes one of the four operational risk causes, the main concern is about non IT operational risks such as risks related to inappropriate processes and procedures of a bank’s trading activities

Operational risk is not new, however significant operation risk events in recent years in the banking industry have highlighted the need to manage operational risk more effectively. In the past, banks had a narrow view of Operational Risk. Today, a broader and more holistic approach is taken. Of course technology and operations issues continue to be important. But operational losses are not solely a result of these operations failures. They arise from breakdowns in other areas. Examples include losses from policy breaches, rogue traders, inadequate or inappropriate documentation resulting in credit losses or customers avoiding their obligations, abandoned projects or external factors.

Increasingly, banks look at the impact Operational risk has on sustainable share value creation or destruction; in turn this is driving a greater shareholder value creation to capture data. Failure to manage risk can lead to other risks and losses e.g. credit provisions and reputational impact such as loss of customers.

According to Don M. Chance (2003), operation risk management should be a process, and not just an activity. The process is continuous and subject to evaluation and revision, and thus constant monitoring and adjustments are required.

Operational risk is a very wide phenomenon that encompasses virtually the risks the Bank may be exposed to. Thus operational risk arises from (but not limited to) the following; crime committed by employees, customers, third parties or a combination of 2 or more of the above, Legal suites by the employees, customers and other third parties, Non-compliance with the central Bank and other laws and regulations, Business interruptions arising from physical disasters, computer systems failure, civil unrest, terrorism among others.

According to Standard Chartered Bank, risk management policy and management of operational risk ranks first in the Bank’s programme, and this is achieved not only through designing procedural manuals but also ensuring that the controls and procedures operate as expected throughout the year on a daily basis without exception. Effective Operational Risk management is an essential part of the bank’s high-level control framework; all staff are responsible for the management and mitigation of Operational Risk

Some tools used in managing operational risk include; Operational audits by internal audit department, Product risk profiles set for each product, service and transaction. The key risk indicators act as red flags to warn on looming danger, operational risk literature keeps top management and employees abreast with current and future risks together with methods of mitigation.

The bank's internal control systems are aimed at minimising risk but these can only succeed if skilled and trusted employees are recruited in the respective areas of operations. The bank is thus an equal opportunity employer which emphasises qualifications, human resources policies and procedures that are available and provide guidelines for recruitment, retention, training, performance appraisal and cessation.

People risk refers to the risk of management failure, organisational structure or other human resources failures. These risks may be exacerbated by poor training, inadequate controls, and poor staffing resources among others.

The risk from processes stem from break downs in established processes, failure to follow processes or inadequate process mapping within business lines.

Systems risk covers instances of both disruption and outright system failures in both internal and outsourced operations.

External events can include aspects such as natural disaster, terrorism, and vandalism.

The range of banking activities and the areas affected by operational risk must be fully identified and considered in the development of the institution's risk management and measurement plans.

Since operational risk is not confined to particular business lines, product types, or organisational units, it should be managed in a consistent and comprehensive manner across the institution. Consequently, risk management mechanisms must encompass the full range of risks, as well as strategies that help to identify measure, monitor and control those risks.

Management should translate the operational risk management frame work into specific policies, processes and procedures that can be implemented and verified with in the institution's different business units. Communication of these elements will be essential to the understanding and consistent treatment of operational risk across the institution.

The operational reporting processes should be periodically reviewed and effective. The institution should have independent verification processes to ensure the timeliness, accuracy and comprehensiveness of operational risk reporting systems, both at the firm-wide and the line of business level.

Independent verification and testing should be done to ensure the integrity and applicability of the operational risk framework, operational risk exposure, and the underlying assumptions driving the regulatory capital measurement process.

2.3. FRAUD

2.3.1. Definition of Fraud

According to Bryan A. Garner, Black's Law Dictionary, Eighth Edition, West Group (2004), Fraud is a broad legal concept that generally refers to intentional act committed to secure an unfair or unlawful gain.

According to Assurance Control and Risk guide for managers (2003), Fraud has no precise legal definition, and thus for the purposes of reporting fraud to the Treasury, the following crimes fall within the context of fraud report; theft though dishonestly appropriating the property of another with the intention of permanently depriving them of it (Theft Act 1968) including the removal or misuse of funds and assets, false accounting through dishonestly destroying and concealing or falsifying any accounts or records with a view to personal gain or gain for another, Bribery and corruption through offering and acceptance of an inducement or reward that may influence the actions taken by the authority (Prevention of corrupt practises Acts 1889 and 1916), Deception through obtaining property or pecuniary advantage by deception(Section 15 and 16 of the Theft Act 1889) and obtaining services or evading liability by deception, Collusion in the context of reporting fraud to treasury to cover any case in which someone incites or attempts to commit any form of crime.

According to the Standard Chartered Bank fraud policy, Standard Chartered Bank is exposed to frauds arising from its daily business/ activities that include but not limited to; savings business, credit/ mortgage business, IT operations, procurement and payments, Human resource procedures, payroll processing, cash processes, cheque frauds, staff activities, conveyance of land among other activities.

Management and the Board shall assess Standard Chartered Bank's level of exposure, prioritize areas of great vulnerability and ensure that proper controls are in place to minimise the exposure.

2.3.2 Causes of fraud

The various causes of fraud identified in the Standard Chartered Bank fraud policy (2007) are categorised into 3 aspects of Financial, attitude towards life and attitude towards the company.

- a) Financial reasons: these include; thinking that you desperately need money, one who does not know how to manage his own money and always runs short of finances and gets tempted to steal , Gambling where one takes some money and is then forced to take more hoping that it will help him to make more money to pay everything.
- b) Attitude towards life; this occurs where one is frustrated or dissatisfied about some aspect of his life, People who are impulsive, distractible and un able to postpone gratification are more likely to engage in fraud.
- c) Attitude towards the company; this involves cases where the employee feels abused by the employer, where employees are not encouraged to discuss personal problems, a feeling by the employee that management is acting in a corrupt manner and thus causing employee disloyalty to the organization, employee believes'' every one steals so why not me'', laxity in controls where one feels that he can get away with it.

According to CIMA, Fraud Risk Management (2007), fraud commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion.

Fraud essentially involves using deception to dishonestly make a personal gain for oneself, or create a loss for another (Fraud Act 2006).

Apostolou et al. (2001) found that management characteristics and influence over the control environment red flags were approximately twice as important as operating and financial stability characteristics red flags and about four times as important as industry conditions using an analytic hierarchy process.

Theory and research suggest that situational effects have a profound effect on ethical behaviour of most people (Dallas 2003). The implication is that it is inappropriate for organisations to rely totally on individual integrity to guide behaviour, and therefore organisations must provide a context that supports ethical behaviour and discourages unethical behaviour.

Moral reasoning is an important element that affects economic decisions made by people, thus facilitating acts of fraud (Rutledge and Karim 1999). Uddin and Gillett (2002) found evidence that moral reasoning had some effect on intentions of Chief Financial officers to report fraudulently on financial statements.

Empirical research suggests that fraud red flags associated with management attitudes and behaviours carry more weight than motivation and condition red flags. There is also evidence that the ethical tone in an organisation is largely from senior management attitudes (Cohen 2002). Research notes that a focus on long term gains and idealist principles should have a positive contribution on reducing earnings manipulation (Elias 2002).

2.3.3. Different types of fraud

Fraud can mean many things and results from many varied relationships between offenders and victims CIMA, Fraud Risk Management (2007).

Examples of fraud include; crimes by individuals against consumers, clients and other business people, employee fraud against employers in form of payroll fraud, falsifying expense claims, theft of cash and misappropriation of other assets, crimes by businesses against investors, consumers and employees, crimes against financial institutions from using lost and stolen credit cards, crimes by individuals or businesses against government through grant fraud and social security benefit claim frauds, crimes by professional criminals against major organisations, e-crime by people using computers and technology to commit crimes through phishing, spamming, copy right crimes, hacking and social engineering frauds.

2.3.4 Methods of fraud detection

According to the study carried out by Price Water House coopers, 2007, various methods of detecting fraud were identified, and these included; whistle blowing hotline, internal tip-off, by accident, external tip-off, law enforcement investigation, change of personnel/ duties, internal audit, external audit, corporate security, risk management.

According to a study by PWC (2007), although external auditors did not detect many cases of fraud, internal auditors on the other hand were found to be the most successful in identifying serious frauds.

Risk management procedures were also found to be one of the most useful methods. If resources would allow it, an organisation should establish a strong internal audit function that monitors and advises on risk management and actively looks for instances of fraud.

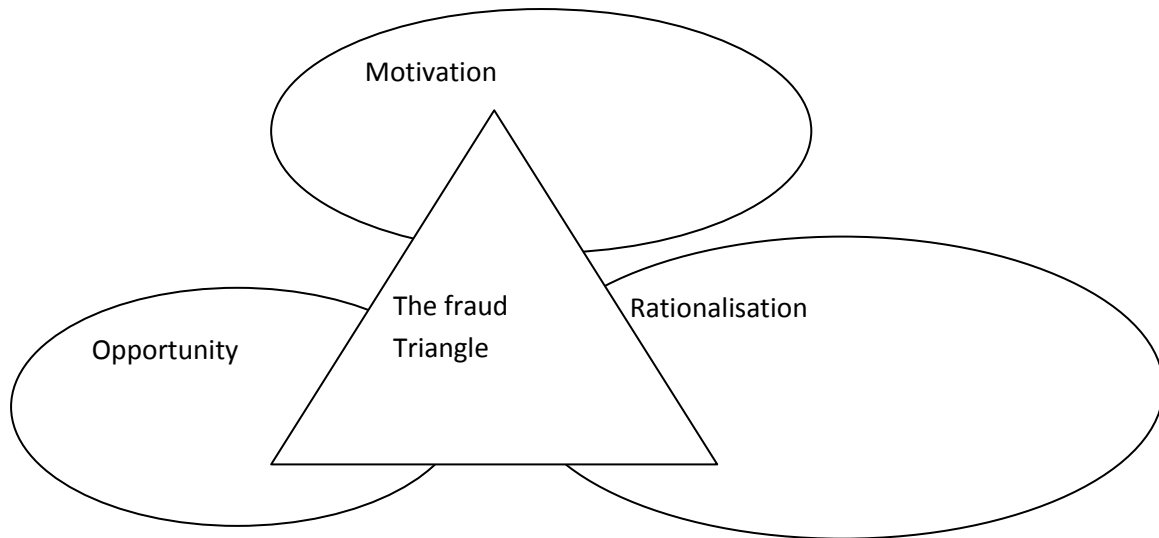
Past studies have shown that having a whistle-blower hotline, internal audit department, surprise audits and fraud awareness or ethical training can cut fraud related losses by half. Thus strong anti-fraud programmes do not guarantee that the company will not be a victim of fraud, it clearly results in a decrease in the losses being experienced, Moses Ssebugwawo (2010).

Fraud may also be discovered as a result of controls and mechanisms put in place on the advice of internal and external auditors.

A lot of frauds, however are discovered accidentally or as a result of information received either via tip off or through a whistle blowing hotline. In many cases, greater losses are suffered as a result of employees at all levels ignoring the obvious.

It's thus every one's responsibility to find and report fraud and irregularities within an organisation, and it is therefore essential that an organisation has an appropriate reporting mechanism in place to facilitate this.

Figure 2.1. The fraud triangle



Source: CIMA, Fraud risk management (2007)

Motivation is typically based on either greed or need.

Recent Fraud surveys have identified greed to be the main cause of fraud. Other causes cited included problems from debts and gambling. Some people with good objective principles can fall into bad company and develop tastes for the fast life, which tempts them to fraud.

In terms of opportunity, fraud is more likely to occur in companies where there is a weak internal control system, poor security over company property, little fear of exposure and likelihood of detection, or unclear policies with regard to acceptable behaviour.

Many people may be able to rationalise fraudulent actions as: necessary-especially when done for the business, harmless because the victim is large enough to absorb the impact, justified because the victim deserved it or because they were mistreated.

According to the Assurance control and risk guide for managers (2003), fraud prevention involves more than merely compiling anti-fraud policies. It also involves putting in place effective accounting and operational controls and maintenance of an ethical environment that encourages staff at all levels to actively participate in protecting public money and property.

Creating an anti-fraud culture involves; having a clear statement of ethical values, establishing a clear anti-fraud policy and fraud response plan, Promoting staff awareness of fraud, Recruitment of honest staff and maintaining of good staff morale.

A number of frauds come into light because of suspicions aroused by, for example the behaviour of certain individuals.

Managers and staff should be alert to any warning signs that might indicate that fraud is taking place, and these may be; staff under stress without a high work load, First to arrive in the morning and last to leave at night, a risk taker or a rule breaker, Reluctance to take leave, Refusal of promotion, unexplainable wealth, sudden change of life style, new staff resigning quickly, cosy relationships with suppliers/ contractors, Suppliers/ contractors who insist on dealing with one particular member of staff, disgruntled at work, greedy member of staff who always express severity financial needs.

The most effective strategies designed to change attitudes to fraud rely on motivation rather than fear. They aim to persuade people of the undesirability at a particular behaviour. Attitude changing strategies rely to a large extent on publicity campaigns to achieve their effect so it is important that departments carry out full appraisal of the benefits of any proposed advertising campaign and to establish some way of measuring the outcomes of such campaigns. Departments need therefore to be clear about the objectives and targets of their campaigns.

2.3.5 External Frauds and Forgeries

In a study conducted by the Uganda Bankers Association in 2009, it was established that ATM Cards and PIN frauds arise due to carelessness of customers in safeguarding them while forged cheques are as a result of alteration of amounts and words, and due to negligence or ignorance of tellers not to identify fake or forged cheques, and there are also increased cases of washed cheques, Identity thefts were noted on an increase. Fraudsters masquerading as Directors, Executives by use of fake Identity cards, Forged letters to withdraw money and open accounts, International Money Transfers (Western Union and Money Gram) through hacking of e-mails between the sender and the receiver, Theft by security guards, especially during the evenings when majority of the staff have left the premises, fake notes, where tellers have been fooled into accepting fake foreign currency notes in exchange for local currency. Fraudsters have succeeded due to negligence and ignorance of the tellers

2.3.6 Internal Frauds and Forgeries

According to a study by the Uganda Bankers Association in 2009, the various forms of internal frauds and forgeries included; Suppression of deposits, where Tellers receive deposits from customers but do not credit customer accounts, or credit customer accounts with a lower deposit value, introduction of false transactions, to hide shortages that have occurred especially in cash, Information Technology (I.T) frauds, through the misuse of staff I.T user rights, Non-compliance with procedures, Bribes, to influence loan applications especially with the clients that lack proper credit worthiness

2.3.7 Other forms of fraud

According to the Ten (10) scandals that rocked Accounting world 2009 Journal, a number of scandals rocked the accounting world, and these include the following amongst others;

i). Enron, which was the most popular and is still being referred to even after 8 years. This scandal involved hiding debts, inflating revenues and corruption. It resulted into the displacement of more than 20,000 people and thus the death of America's most innovative company for six years and the dissolution of one of the Big 5 global accounting firms (Arthur Andersen).

ii). Parmalat is another company based in Italy. Parmalat used to be the biggest dairy company in Europe but it collapsed in 2003 and subsequently declared bankrupt. The company went bankrupt for a number of reasons; as investment disaster, nonexistence of cash in the Bank, fake transactions, hidden debts, and the use of derivatives and accounting fraud to hide these facts. These illegal acts were carried out worldwide, and they affected not only the company and its people but international financial institutions as well.

iii). World com is now known as MCL, Inc .and is part of the Verizon Communications group. The company emerged from bankruptcy in 2003. Fraud was committed in the World com through inflating assets and revenues, understatement of operating expenses and liabilities. World com chapter of bankruptcy filing is second next to the Lehman Brothers in 2008 in the history of such filings in the USA.

iv). Tyco international limited- an international manufacturing company with diversified product lines (safety products, fire protection and electrical products, to name a few). The fraud actually involved misuse of the company's funds by its former Chief Executive Officer (CEO), and Chief finance officer (CFO). They utilised improper accounting practises to cover up the misuse of these funds.

2.4. The relationship between operational risk management and combating of fraud in banking institutions

According to the Assurance, control and Risk guide for managers by HM Treasury, UK (2003), the risk environment is constantly changing and priorities of objectives and the consequent importance of risks on the fraud risk profile will shift and change. Risk models have to be regularly revisited and reconsidered in order to have an assurance that the fraud risk profile continues to be valid. Control systems should be revisited at regular intervals and in particular after restructuring, downsizing, changes in business processes, following identification of weaknesses, the introduction of new computer systems and after an incident of fraud. The risk of fraud should be considered along with other risks when major new policies are being developed, where a change in policy occurs or where changes are made to the way in which policy is to be implemented.

Fraud is just one of the many risks an organisation faces. However the deliberate nature of fraud can make it difficult to detect and to deter.

Risk in the context of managing fraud risk is the vulnerability or exposure an organisation has towards fraud and irregularities. It combines the probability of fraud occurring and the corresponding impact measured in monetary terms. Preventive controls and the creation of the right type of corporate culture will tend to reduce the likelihood of fraud occurring while detecting controls and effective contingency planning can reduce the size of any losses.

A risk based approach enables organisations to target their resources, both for improving controls and for pro-active detection, at problem areas. Developments in corporate governance, including the requirement for statements on internal control, create the atmosphere in which fraud can be considered as a set of risks to be managed alongside business risks. Managing the risk of fraud should be embedded in the entirety of an organisation's risk, control and governance procedures.

Managing the risk of fraud involves; assessing the organisation's overall vulnerability to fraud, identifying the areas most vulnerable to risk of fraud, evaluating the scale of fraud risk, responding to the risk of fraud and measuring the effectiveness of the fraud risk strategy.

According to the new vision, Uganda, National daily of the 26th February 2010, Moses Ssebugwawo stated that, fraud prevention starts with risk assessment, as many executives in Uganda today believe that their companies have strong programs in place to prevent fraud, mostly referring to the code of conduct that has to be signed by all employees. However we continue to see pictures of individuals wanted by police over theft of company money and property every day in the newspapers.

This gives a direct signal that companies are experiencing increased cases of fraud despite all the control measures put in place by executives of different companies.

He says that while the code of conduct is a necessary and an important element in the fight against fraud, it is far from sufficient. What is thus needed is a robust anti-fraud programme that addresses fraud prevention programs, regular fraud training and communication, fraud risk assessment, fraud control monitoring and a fraud response plan.

Bell and Carcello (2000) presented a model useful in predicting the existence of fraudulent financial reporting which correctly classified 80 percent of the fraud cases while only misclassifying 11 percent of the non- fraud cases. The significant risk factors included in the model were: weak internal control environment, rapid growth, inadequate/ inconsistent profitability, undue emphasis on meeting earnings projections, dishonest or overly evasive management, ownership status (private verses public), and an interaction between a weak control environment and an aggressive attitude towards financial reporting. Bell and Carcello's work shows that there are several risk factors presented in the authoritative guidance and elsewhere in the literature that are not particularly effective in discriminating between fraud and non-fraud engagements.

CHAPTER THREE

3.0. METHODOLOGY

This chapter presents the methods and procedures the researcher employed in the study; it presents the research design, population of study, sample size, sampling methods, sources of data, data collection instruments, pre-testing instruments, procedures for data collection validity and reliability, data management and analysis, measurement of variables and ethical considerations

3.1. RESEARCH DESIGN

The research was a case study research design. This research design helped the researcher control the extraneous variables of the study and assisted the researcher in establishing the relationship between operational risk management and combating fraud in Standard Chartered Bank

3.2. AREA AND POPULATION OF STUDY

The research was conducted at Standard Chartered Bank (SCB). Different departments at the Head office were considered for the research study, these included the operations, credit, risk/audit, marketing including employees in management positions such as heads of departments and section heads at the bank's head office.

3.3. SAMPLE SIZE AND SAMPLING TECHNIQUE

3.3.1 .Sample Size

Much as Standard Chartered bank carries out its activities in 11 branches, that is Speke Road branch, Ndeeba branch, Kikuubo branch, Ntinda branch, Lugogo branch, City branch, Mbale branch, Mbarara branch, Jinja branch, Garden City branch and Gulu branch, the researcher carried out the study at the Speke Road branch due to the fact that bank's head office is located at Speke road and it is where majority of the operational activities and functions are carried out. The departments and functions include; Operations department, the Treasury department, Credit department, Audit/ risk department, Marketing, ATM operations section and Finance department

The reason why the researcher used Speke Road branch was because it is nearer and she had other duties to carry out which made it impossible for the upcountry branches to be included in the research.

Since it is not cost effective to study the whole targeted population (Mugenda and Mugenda, 2003), sampling was done. The sample size was estimated depending on the resources of time

and money at the researcher's disposal. For this study the sample size was 50 respondents that were approached for the study

Table 3.1: Distribution of respondents per department

	Departments	Number of respondents	Population size
1	Operations	20	50
2	Treasury	6	10
3	Loans	8	20
4	Audit/Risk	10	30
5	Retail	6	35
	Total	50	145

Source: Primary data

Standard Chartered bank was selected for the study because it provided the required personnel that availed the researcher with the necessary information required for the study.

The respondents included both junior and senior employees of Standard Chartered bank. This played an important role in ensuring that no vital information was left out

3.3.2 Sampling Technique

The respondents were drawn from the various categories of staff by using simple random sampling technique that was employed to select the junior staff from each department. Simple random sampling was employed to ensure that bias is avoided in the selection of respondents. A purposive sampling technique was employed in the selection of senior staff members from the various categories who are experienced and knowledgeable in this field of study. This technique was used to ensure that all the different categories of employees were chosen purposively and all grades of workers of Standard Chartered Bank were fairly represented.

3.4. SOURCES OF DATA COLLECTION

The researcher employed both primary and secondary sources of data

3.4.1. Primary Sources

The researcher used a questionnaire to gather the necessary data from the respondents. Under this method, structured questions were developed and administered to the respondents. Both closed and open ended questions about the impact of operational risk management strategies in combating fraud in Standard Chartered bank were sent to the selected employees of Standard Chartered Bank

The questionnaire instrument was used because it is simple to administer and Questionnaires can be easily filled in by the respondents at their most convenient time.

Unstructured interviews were also used as another source of primary data collection.

This method gave the respondents convenient time to sit down and fill in the questionnaire or fill it in at any other time of their choice.

3.4.2. Secondary Sources

The researcher further extracted data from library newspapers, business journals, and reports on employee performance. Data collected from secondary sources was collaborated with the first-hand information from the primary sources so as to come up with a conclusion. Other secondary data source, documentary and archival method were used. This involved reading and analysing the written down operational policies and procedures of Standard Chartered bank and various reports that were found to have a bearing on the operational risk management in the combating fraud. Such reports included; audit reports, risk and compliance reports, management reports, reconciliation reports, and customer transaction analysis reports, reports from regulators (Bank of Uganda) and among others.

3.5 .VARIABLES UNDER STUDY

The variables for the study are risk management and Fraud. Risk management is the independent variable and Fraud is the dependent variable. The researcher concentrated on how fraud in banking institutions like Standard Chartered Bank is dependent on poor risk management strategies and therefore these variables were used as a yardstick in analysing the impact of operational risk management strategies in combating fraud in Standard Chartered Bank

Dependent Variable(Y) =Function (Independent Variables)

Fraud(Y) =F (systems, people, Technological changes, internal controls, losses from policy breaches, inadequate or incorrect documentation, launching of new products without adequate operational support, low levels of ethics and integrity)

3.6 DATA MANAGEMENT AND ANALYSIS

3.6.1. Data management

The study instruments used yielded both qualitative and quantitative data. After the respondents have answered the questions and interviews, raw data was cleaned, edited, coded, and sorted for consistency, uniformity and accuracy.

3.6.2. Data Analysis

The coded responses were then entered into a computer using S.P.S.S (Statistical Package For social scientists) to analyse the findings of the study and find a diverse level of variables like age, sex, work experience and exposure of the respondents. The findings of the study are presented in graphs and pie charts. The decisions were made basing on highest percentages and frequencies from the primary data gathered to establish the role of operational risk management strategies in combating fraud in financial institutions

3.7. PROCEDURE OF THE STUDY

The study was carried out in an organized way; a pre-test on the research instruments such as questionnaires was made, to ascertain whether they would collect the desired information.

These instruments were thus pre-tested for validity and reliability and this was helpful in instilling confidence in the respondents.

Questionnaires were sent to the respondent and filled, they were later collected after being filled. These questions were focused at establishing the relationship between operational risk management and combating of fraud in banking institutions.

3.8. LIMITATIONS OF THE STUDY

During the research, the researcher was faced with a number of challenges and these included the following;

- Delays by the respondents in returning the questionnaires as they found it time consuming given their tight work schedules. This affected the researcher's turnaround time
- A financial limitation as the research was self-sponsored.
- Creating time for the research was a problem as the researcher had to carry out the research during working hours

Despite the above problems encountered during the research, it was a success due to co-operation from all the staff that were approached for the study

CHAPTER FOUR

4.0 DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS

This chapter presents findings about the study. The findings are both qualitative and quantitative and are summarised from mainly primary data and presented in tables and charts. The relationship between the variables is ascertained by correlation and regression analysis. The findings are interpreted in relation to the research objectives and the research questions.

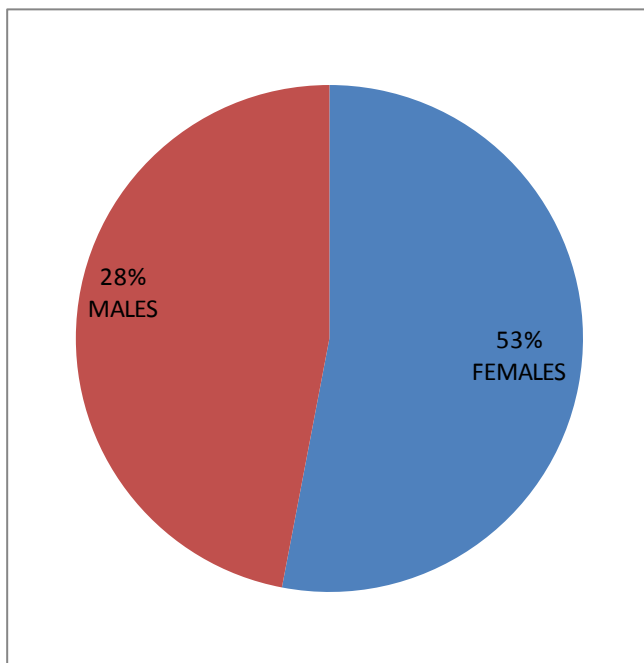
4.1 DEMOGRAPHIC CHARACTERISTICS

In the study only Speke Road branch was visited and 50 respondents were selected for the study.

4.1.1 Distribution of respondents by sex

The study covered 50 respondents out a population of 453 staff .Out of the 50 respondents interviewed, 53% were females and 47% were males

Figure 4.1: Percentage distribution of respondents by sex



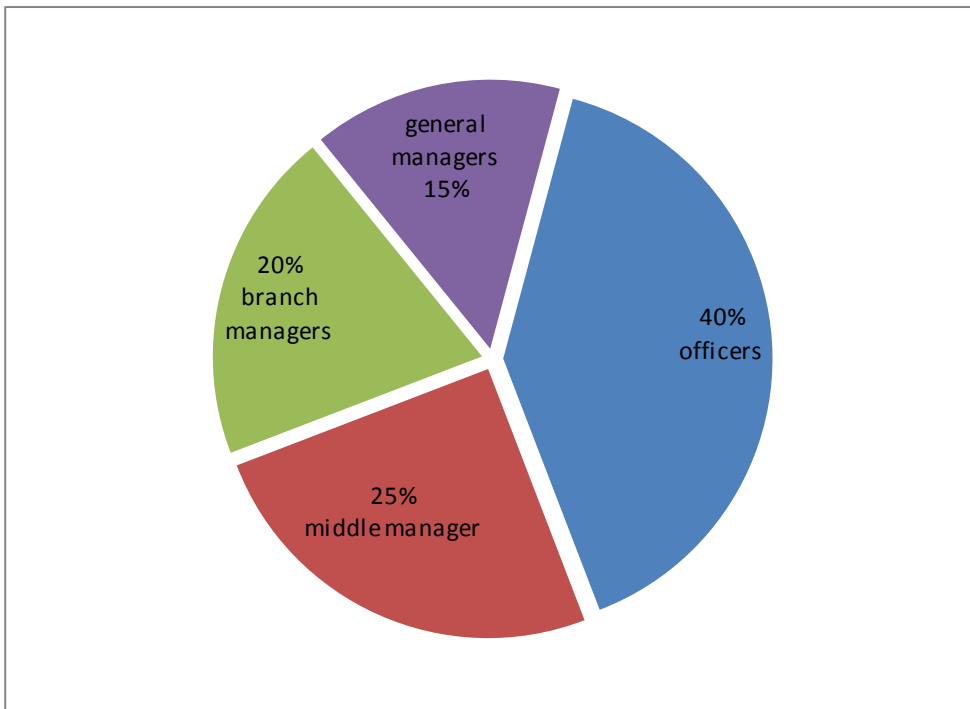
Source: Primary data

4.1.2 Distribution of respondents per role

Of the 50 respondents, 40% of the respondents were officers, 25% were middle managers, 20% were Branch managers and 15% were General managers of various departments of Standard Chartered Bank that are exposed to the risk of fraud.

Majority of the respondents were officers who are in most cases aware of the risk of fraud in banking institutions.

Figure 4.2 Percentage distribution of respondents per role



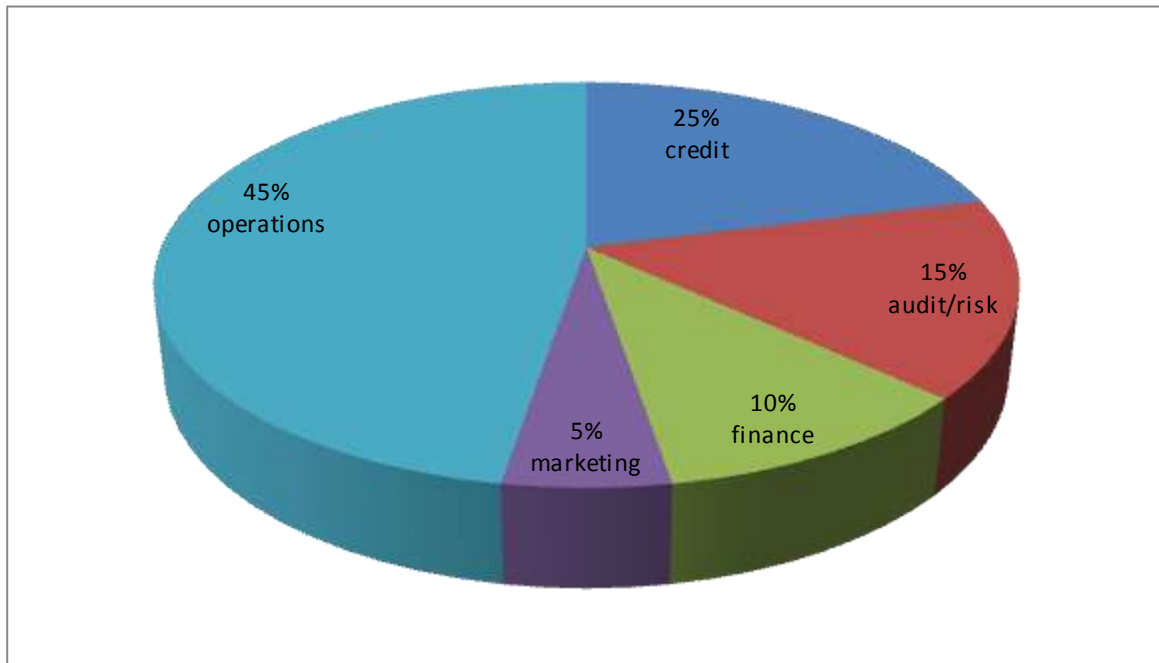
Source: Primary data

4.1.3 Distribution of respondents per department

The results in the figure below indicate that, 25% of the respondents were from credit, 15% were from audit/risk, 45% were from operations, 5% were marketing and 10% were from finance departments.

This implied that the majority of the respondents were directly involved in operational risk management processes and hence had vast knowledge about the impact of operational risk management in mitigating fraud in standard Chartered bank

Figure 4.3 Percentage distribution of respondents per department

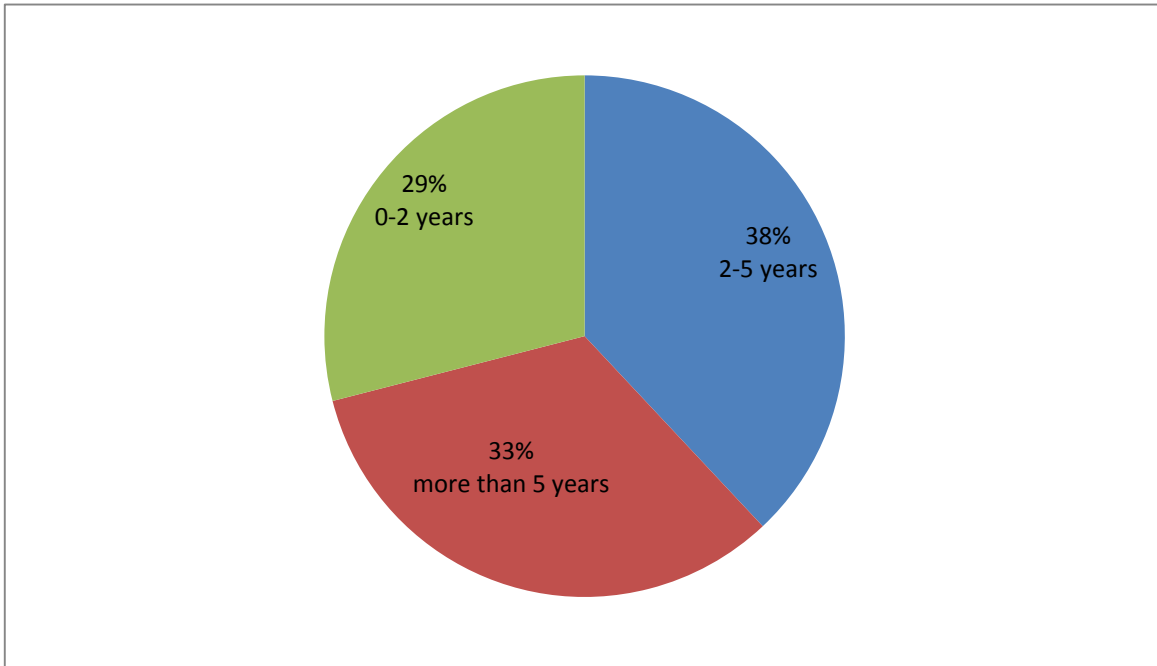


Source: Primary data

4.1.4 Number of years spent in the department

From the study it was discovered that majority (71%) of the respondents had worked in their respective departments in Standard Chartered bank for more than 2 years. This implied that majority of the respondents had experience in extending banking services to the various stakeholders for some time and were aware of the operations of Standard Chartered bank.

Figure 4.4 Percentage distributions of Respondents by number of years in the department



Source: Primary data

4.2 INFERENTIAL STATISTICS

4.2.1 The impact of operational risk management in combating fraud

This was looked at in terms of programs and procedures that aim at creating operational risk awareness in combating fraud, how the programs are conducted, whether the programs have had any impact in combating the risk of fraud in Standard Chartered bank.

The results in the table below indicate that 92% of the respondents believe that operational risk management has an impact in combating the risk of fraud in Standard Chartered bank.

Respondents replied that Standard Chartered bank has programs that aim at creating operational risk awareness in combating fraud, and these programs include operational procedures, training activities, awareness programs, workshops and seminars among others.

Table 4. 1 The impact of operational risk management in combating fraud

	Frequency	Percentage (%)
Has impact on fraud	46	92
Has no impact on fraud	4	8

Source: Primary data

The respondents also indicated that the programs have had a great impact in mitigating the risk of fraud in Standard Chartered bank, and thus fraud cases have reduced to a minimal level, customers have gained confidence in the bank, perpetrators of fraud can easily be identified, employees have become more vigilant while handling customer transactions, suspicious transactions can easily be identified among others.

The respondents however indicated that awareness programs, seminars and workshops are sometime co-ordinated by people who lack hands on experience in banking operations, and sometime people identified to participate in these programs are people from departments that are not exposed to the risk of fraud. Such departments include, marketing, Audit and Risk departments

Most of the respondents (90%), said that most frauds faced by banking institutions are perpetrated by the members of staff, and thus workshops, seminars and awareness programs may have no impact in combating the risk of fraud.

The study further revealed that, some employees at lower levels are not given platform to share their experiences as they execute their day to day duties, and yet most of the activities they carry out in the bank are vulnerable to the risk of fraud.

4.2.2. The relationship between operational risk management and fraud

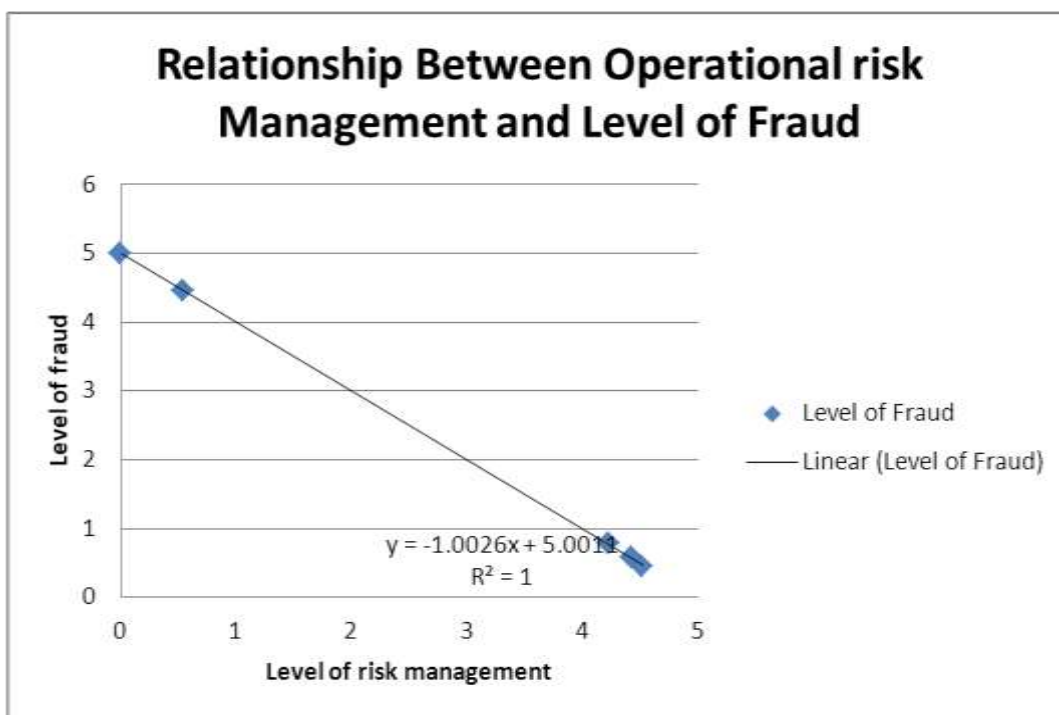
Pearson correlation coefficient was employed to establish the relationship between operational risk management and fraud. Operational risk was an independent variable and the dependent variable was fraud. Levels of risk management and fraud were assessed on the following parameters.

- The Operational environment
- The people through un authorised trading, insider dealing, organised labour activity, employee illness and injury etc.
- The systems through hardware and software failure, un availability and questionable integrity of data, un authorised access to information and system security, Telecommunication failure, computer hacking or viruses
- Process risk in the form of breach of mandate, incorrect or untimely transaction capture, loss of client assets, mispricing of products, accounting and taxation errors, inadequate record keeping, corporate action errors
- Risk from external events through operational failure at suppliers or out sourced operations, fire or natural disaster, Terrorism, Vandalism, pilferage, theft and robbery etc.

Table 4.2 Level of risk management and fraud

Parameters	Level of Risk Management	Level of Fraud
i	4.52	0.45
ii	4.23	0.77
iii	0.54	4.46
iv	0	5
v	4.43	0.57

**Correlation= -0.99998593
coefficient**



The correlation coefficient(r) of - 0.99998593 in the correlation above indicates that there was a significant negative relationship between operational risk management and the risk of fraud. This implied that a higher level of operational risk management contributes lowers the risk of fraud in the banking institutions.

At institutional level, it was found that operational risk management tools such as the internal controls, processes and procedures, operational policies and manuals are translated into reduced levels of the risk of fraud in the banking institutions.

Therefore banking institutions should focus on strengthening operational risk management measures so as to minimise the risk of fraud.

4.2.3. The effectiveness of operational risk management in combating fraud

The effectiveness of operational risk management in combating fraud was assessed in terms of determining whether Standard Chartered bank has written operational, risk and fraud policies that guide in the day to day operational decisions. Majority of the respondents (98%) agreed that Standard Chartered has operational risk and fraud policies and manuals in place that assist in the creation of awareness to employees and other stakeholders on the best practises, procedures and processes to be followed, methods of fraud detection, disciplinary actions against perpetrators

When assed on how useful these policies and manuals are, 86% of the respondents strongly believe that operational risk management is effective in mitigating the risk of fraud in Standard Chartered bank, and these risk and fraud policies and manuals are reviewed periodically every after 24 months and at times when a need arises.

They said that review of the policies and manuals is carried out by mainly supervisors and managers, although various officers at lower ranks too make contributions towards the reviews.

This implied that timely reviews of the manuals and policies would allow updates to be made about any developments in the methods of detecting and combating the risk of fraud.

Table 4.3 The effectiveness of operational risk management in combating fraud

	Yes (VU,S &FU)		No (P & N)	
	%	frequency	%	frequency
Is effective in combating fraud	86	43		
Not effective in combating fraud			14	7

Source: Primary data

VU: Very useful, S: Useful, FS: Fairly useful P: Poorly, N: Not Sure

The study also revealed that 14% of the respondents were not sure about the key elements of operational risk such as people, system failures, processes, risks from external events, and the roles they play towards contribution to the risk of fraud. 72% of the respondents indicated that there have been some cases of fraud in Standard Chartered bank, though most have been immaterial, and these have been in line with suppression of customer deposit, forgery of customer signatures. These forms of frauds were found among the members of staff who were reluctant to take leave, refused to take promotion, staff who suddenly changed their life style, staff with cosy relationship with suppliers and contractors among others.

Respondents also indicated that other methods of fraud detection in banking institutions include whistle blowing, internal tipoff, by accident, internal audit, and external tipoff among others.

4.2.4. Other creative techniques of operational risk management explored to combat fraud to an acceptable level

The results shown in the table below indicate that majority of the respondents (88%) indicated that various operational risk management measures help in combating the risk of fraud. Among the measures identified were; introduction of an ethics policy statement, introduction of a fraud policy statement, introduction of a fraud education, training and awareness programs, introduction of a whistle blowing policy, constant review of all anti-fraud policies and programs.

Table 4.4 Creative measures of operational risk management in combating fraud

	Frequency	Percentage (%)
Measures combat fraud	46	88
Measures do not combat fraud	4	12

Source: Primary data

The respondents replied that some measures such as the ethics policy statement, fraud policy statement, whistle blowing policy were not very clear to them at the time they were introduced to the bank, up to the time of their implementation. This however resulted into some information gaps among some employees and thus increasing the vulnerability of the risk of fraud in Standard Chartered bank.

82% of the respondents indicated that the bank has a fraud prevention plan, and it's thus committed to combating the risk of fraud.

The respondents also indicated that once fraud by a member of staff or customer has been detected, it's reported to the supervisors, who investigate it further, and once perpetrators of the fraud are identified, they are terminated from employment and they are eventually blacklisted.

4.2.5 Other opinions about operational risk management and fraud

From the study, the respondents pointed out that, despite various interventions such as effective safe guards and internal controls, anti-money laundering policies, know your customer campaigns and emphasis on best practices, frauds have persisted in banking institutions due to a number of reasons;

- Fraud perpetrated by internal members of staff is also difficult to detect, and much as safeguards may be put in place, they can easily be compromised by internal staff members, and thus making fraud persistent.
- Some Banks do not expose fraudsters to the public, once a fraudster is identified; they are only punished without alerting other players about the actions committed by such a person. Even when other banks publicly expose the fraudsters, other banks may not easily get to know about it as they have no access to the database that can be used to make references about people who may be under investigation.
- Low motivation among members of staff, can make fraud to persist, especially with the staff members who may feel that they are rewarded less in relation to their productivity or level of output to the banks.
- Banks also invest into new products without carefully investigating how vulnerable they can be to fraud during implementation.
- Lack of training and awareness programs. Banks have become adamant to offer training and sensitization programs, aimed at equipping skills of detecting and mitigating fraud. Even when the programs are in place, they are not designed and facilitated in a way members of staff can easily understand.
- Low levels of ethics and integrity. This is common among the fraudsters by their nature, and thus whatsoever much the employers attempt to motivate them, they will continue to be fraudulent.
- Employees getting used to a particular operational activity, without getting exposed to other functions in the organization, thus leading to supervisors to develop a lot of trust in the employee to the extent of ignoring routine control checks and audits.
- System failures in the banking institutions can also facilitate fraud. This is common with systems that lack proper controls. An example identified by respondent was with banks that offer ATM services to customers. System failures can make it possible for customers to over draw their bank accounts without any authority.
- Lack of Technological advancements. Some Banks are reluctant to invest in robust information Technology systems that have controls that can help combat the risk of fraud. This is because such systems are usually too expensive, and banks may not be willing to make huge investments in such systems.

- Aggression by members of staff has also made fraud persistent. This has been common among members of staff who operate on a slogan of get rich quick syndrome. Most of these members of staff tend to live beyond their means.

CHAPTER FIVE

5.0. SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

This chapter presents a summary of major findings, conclusion and recommendations arising out of the research findings.

5.1 SUMMARY AND CONCLUSION

Despite meeting a few impediments during the course of the study, the research was a good experience and important exercise to the researcher

Despite the fact that banking institutions have the ability to combat the risk of fraud, they are still faced with a number of challenges in the process which limits their ability to operate in a healthier banking environment, and thus they continue making losses and their reputation is at risk as a result of the failure to effectively combat fraud.

Some of the major challenges faced by banking institutions include; frauds mainly perpetrated by the internal staff, high costs of investing in robust information technology software, high costs of training, most banks are regulatory driven, and thus are putting in place measures because it is required by the regulator, other banks take up training programs because industry leaders (the big banks) have taken them up, unmotivated staff and failure by the staff to live within their means.

The study was carried out in Standard Chartered bank. Speke road branch was used for the study and a total of 50 respondents were interviewed for the study.

The research was carried out to establish the role operational risk management strategies in combating fraud in financial institutions, specifically Standard Chartered Bank. The findings of the study are summarised basing on the research objectives as shown below;

The study was to establish the impact of operational risk management in combating fraud. From the study it was found out that operational risk management has a great impact in combating the risk of fraud in banking institutions. Failure to implement the operational risk management programs makes fraud in banking institutions persistent.

The relationship between operational risk management and fraud was that there is a significant negative correlation between operational risk management and fraud ($r = -0.99998593$), hence the risk of fraud reduces greatly as operational risk management measures are strengthened

In assessing the effectiveness of operational risk management in combating fraud, the study revealed that operational risk management is effective in combating the risk of fraud in the

banking institutions. Respondents have a strong belief that there is need to improve on the operational environment through putting in place effective safeguards and controls, transaction monitoring to identify suspicious transactions, timely review of policies and manuals and involvement of staff at all levels in the review of the policies and manuals in order to have more effectiveness in combating the risk of fraud.

In exploring creative measures of operational risk management in mitigating fraud, the study revealed that in banking institutions there are various measures that can be employed to combat the risk of fraud. It is therefore very important for banking institutions involve employees at all levels in coming up with measures aimed at combating the risk of fraud, so that they get a better understanding of how such measures operate and effectively participate in the effort to combat the risk of fraud.

5.2 RECOMMENDATIONS

This study was designed to find out the role operational risk management strategies in combating fraud in financial institutions. Despite the operational risk management strategies that banks have in place, they have continued to lose funds through frauds. Basing on the findings of the research, the recommendations below are crucial for banks to maintain a good ethical track record and zero tolerance to fraud;

- The findings of the research revealed that there is a negative correlation between operational risk management and fraud. therefore banking institutions need to place more emphasis on reporting of information aggregated by risk category to business line management, risk committees and the board, education and involvement of staff and personnel in designing and implementation of programs aimed at mitigating fraud, periodic and timely reviews of policies/ manuals and daily suspicious transaction monitoring.
- For operational risk management to be more effective in combating fraud in financial institutions and in particular Standard Chartered bank, management should emphasize timely review of the manuals and policies in order to keep updated on any new changes regarding the methods of fraud detection and prevention.
- The study revealed that some employees at lower levels are not given platform to share their experiences as they execute their day to day duties, and yet most of the activities they carry out in the bank are vulnerable to the risk of fraud. Therefore for banking institutions to be able to combat the risk of fraud, awareness programs and workshops must be tailor made to fit in the local working conditions of the employees. With effective awareness programs, fraud would be reduced to a minimal level.

- As banks strive to combat the risk of fraud, they should focus on the departments that are directly involved in operational risk activities. This could be done through regular trainings and awareness programs to equip the staff members concerned with the necessary skills for successful mitigation of the risk of fraud. The staff in the various departments should be motivated to encourage them to minimise fraud by being vigilant while attending to customers, reporting any suspicious transactions, emphasising best practises, sharing personal experiences among others.
- The Banking institutions should develop staff training programs, which are fraud detection and mitigation oriented in order to equip the staff with the skills necessary for successful detection and minimisation of fraud.
- Banking institutions should hold awareness seminars and workshops to sensitize their employees' strategies of mitigating the risk of fraud on a regular or weekly basis.
- Banking institutions should establish and maintain public confidence in their services. Public awareness could be improved through seminars, workshops and the use of appropriate advertising media.
- Counselling and openness by management to other members of staff must be done at timely intervals in order for all members of staff to have loyalty to their employer at all times in order to reduce the risk of fraud.
- Risk management must be centred on identifying cases of internal fraud as a starting point, as most frauds reported in various banking institutions are mainly perpetrated by the internal members of staff.

- In their drive to combat the risk of fraud, banking institutions should put emphasis on departments that are directly involved in operational risk activities. This could be done through regular trainings and awareness programs to equip the staff members concerned with the necessary skills for successful mitigation of the risk of fraud. The staff in the various departments should be motivated to encourage them to minimise fraud by being vigilant while attending to customers, reporting any suspicious transactions, emphasising best practises, sharing personal experiences
- In order to improve on the operational environment, Standard Chartered bank should put in place effective safeguards and controls, transaction monitoring to identify suspicious transactions, timely review of policies and manuals and involvement of staff at all levels in the review of the policies and manuals.
- Banking institutions, in particular Standard Chartered banks should always consult lower employees when designing operational risk management strategies. This could be through conducting surveys, sticularharing experiences, best practises and carrying out awareness programs.

Lastly but not least, the respondent indicated that various measures can be put in place to help combat the risk of fraud and these are among others;

- Staff motivation, in the form of increased job benefits and alignment of staff remuneration with work done and profitability of the bank.
- Operational processes and procedures should periodically be reviewed
- Continuous and vigilant transaction monitoring.
- Banks must put in place effective safeguards and internal controls.
- Banks should properly train staff.
- The best practices in banking should be emphasized among all employees
- Proper documentation and record keeping.
- Know your customer (KYC) campaigns should be emphasized to eliminate fraudulent customers
- Banks should adopt high technology banking software
- Emphasis on ethical behaviour among the members of staff.
- Stronger punishment should be administered to the perpetrators of fraud in form of dismissal from work and blacklisting them in connection with high level crimes

- Increased vetting of customers by the use of institutions such as the credit reference bureaus.
- All transactions on bank ledgers and customer accounts should be reconciled on a daily basis.
- Increased collaboration, sharing of information and experiences among banks with in the banking fraternity.
- Human resources should do proper employee screening during the recruitment exercise
- Promotion of whistle blowing and need to maintain confidentiality of the whistle blowers.

REFERENCES

The new Basel capital accord (NBCA), known as Basel II

Basel committee on banking supervision, revised Framework of international Convergence of Capital Measurement and Capital Standards-June 2004 p.g 137

R.P Naita, (2005), Banking System, Frauds and Legal Control.

Nabhan, Reem Abdul Latif, Hindi, Nitham M (2009); Bank fraud: perception of bankers in the state of Qatar, academy of Banking Studies Journal

Basel Committee on Bank Supervision (2001) "Operational Risk" www.bis.org

KPMG International (2006), Fraud Risk Management; Developing a Strategy for Prevention, Detection, and Response, URL: http://www.us.kpmg.com/Rutus_Prod/Documents/12/FRM-White-Paper.pdf, Last Accessed: 7th August, 2010.

Vasiu, L, Warren, M & Mackay, D (2003), Defining Fraud: Issues for Organizations from an Information Systems Perspective, URL:<http://www.pacis-net.org/file/2003/papers/is-strategy/175.pdf> , Last Accessed: 7th August, 2010.

Financial Institutions Act (FIA), 2004, URL: <http://www.bou.co.ug>

Onkagba, J.O. (1993): "Auditing computerization information system: A growing audit challenge", *The Nigerian Accountant*, Lagos, Published by ICAN, Jan/Mar.

Diana Thompson (2003), Risk management: A brief history, moneywatch.com / [The Economy Publications](http://TheEconomyPublications.com) / [Journal of Banking and Financial Services](http://JournalofBankingandFinancialServices.com) / June-July, 2003 issue, URL: http://findarticles.com/p/articles/mi_hb3252/is_3_117/ai_n29013716/, Last accessed: 6th August 2010

CFA Institute, Global Association of Investment Professionals, URL: <https://www.cfainstitute.org/about/investor/cfaglossary/Pages/index.aspx?SelectedLetter=R>, Last Accessed: 8th August 2010

Godfrey, P. S, (1997) Control of risk a guide to the systematic management of risk from construction.

De Greuning, H. (2006). Analiza și managementul riscului bancar, Editura Irecson

Edna Stan-Maduka, (2009) University of East London; Operational Risk Management In Banks

Buchelt, R. and Unteregger, S. (2004). Cultural risk and risk culture: operational risk after Basel II. Financial Stability Report 6, URL: http://www.oenb.at/en/img/fsr_06_cultural_risk_tcm16-9495.pdf, Last accessed: 6th August 2010

Halim Alamsyah, (2008), Poor Operational Risk Management can lead to losses at Banks, Conference in Jakarta-Indonesia, URL:http://www.jltasia.com/media/press_releases/2008/20081119_Poor_OpRisk_can_lead_to_losses_at_Banks.pdf, Last accessed: 7th August 2010

Don M. Chance, (2003), Analysis of Derivatives for the CFA program

Supervisory Guidance on Operational Risk Advanced Measurement Approaches for Regulatory Capital, (2003), URL: <http://www.fdic.gov/regulations/laws/publiccomments/basel/oprisk.pdf>, Last accessed: 1st August 2010

Smith, RG (2001), 'Defining, Measuring, and Reporting Fraud Risk Within Your Organisation' in *Applying Risk Management to Implement a Proactive Fraud Prevention Strategy in Financial Services*, I.I.R. Conferences, Parkroyal Darling Harbour, 19-20 July 2001, URL: http://www.aic.gov.au/conferences/other/smith_russell/2001-07-IIR.pdf Last accessed: 1 August, 2010.

Chartered Institute of Management Accountants (CIMA) (2008), *Fraud risk management, a guide to good practice*, Second edition.

Spam laws, URL: <http://www.spamlaws.com/fraud.html>, Last accessed: 19th July, 2010

The risk management process flow chart, URL: http://www.scu.edu.au/risk_management/index.php/2/; accessed on 19th August, 2010

Aviation safety, URL: <http://www.wildfirelessons.net/Additional.aspx?Page=181>, last accessed: 19th August, 2010

The Ugandan Banker, vol 15. September 2006 issue. ISSN 1605-7848

Christopher Kigenyi (2006), *Managing Risks in Financial Institutions*. The sixth east African Banking School

APPENDIX A

MAKERERE UNIVERSITY

COLLEGE OF BUSINESS AND MANAGEMENT SCIENCES

QUESTIONNAIRE FOR THE STAFF OF STANDARD CHARTRED BANK

I am a student from Makerere University pursuing a masters' degree in Business Administration, i am carrying out research on the role of operational risk management strategies in combating fraud in financial institutions; with emphasis on banking institutions. Your institution has been selected as the case study and i kindly request you to spare some time and answer the questions contained in this questionnaire

The information obtained will be used solely for academic purposes and thus the recommendations may therefore be beneficial to your institution. Your responses will be treated with utmost confidentiality.

Topic: "The role of operational risk management in combating Fraud in Financial Institutions. - A case study of Standard Chartered Bank Uganda Limited. "

SECTION ONE: BIO DATA

Please tick or fill in the spaces where appropriate

1. Gender i) Male ii) Female

2. Please indicate your educational background

i) Certificate level ii) Diploma iii) Degree

iv) Others (specify) _____

3. Which of these titles do you hold?

i) General Manager ii) Middle manager iii) Branch Manager iv) Officer

v) Others specify _____

4. To which department do you belong?

i) Operations ii) Audit /risk iii) Credit iv) Finance v) Marketing

vi) Others, specify-----

5. For how many years have you been in this department?

- i) Less than 2 years ii) 2-5 years iii) Above 5 years

SECTION TWO: TO ASSES THE EFFECTIVENESS OF OPERATIONAL RISK MANAGEMENT IN COMBATING FRAUD

Please fill in by ticking the appropriate options given

6. Do you have written operational, risk and fraud policies/manuals that guide you in your day to day operational decisions in your institution?

- i).Yes ii) No

7. If yes, how useful are these policies in;

	Very useful	useful	Fairly useful	Poorly	Not sure at all
Assessing the impact of operational risk management in mitigating fraud					
Formulating the basic principles of operational risk management					
Establishing the relationship between operational risk management and fraud					
Establishing the extent to which operational risk management has contributed to reduction of fraud in Standard Chartered Bank.					

8. Are the policies/manuals in No.6 above periodically reviewed?

- i).Yes ii) No iii) Not aware

9. If yes, how often are they reviewed?

- i) Every year ii) Every 2 years iii) Every 5 years

iv) Others (specify)_____

10. Who is in charge of carrying out the review of the policies/ manuals?

- i). Tellers ii) managers iii) Supervisors

iv). others, please specify-----

Please answer by filling in the most appropriate options given

11. How crucial is the following towards contribution to operational risk in Standard Chartered Bank?

	Very crucial	crucial	Fairly crucial	Hardly crucial	Not crucial
The Operational environment					
The people through un authorised trading, insider dealing, organised labour activity, employee illness and injury etc					
The systems through Hardware and software failure, un availability and questionable integrity of data, un authorised access to information and system security, Telecommunication failure, computer hacking or viruses					
Process risk in the form of breach of mandate, incorrect or untimely transaction capture, loss of client assets, mispricing of products, accounting and taxation errors, inadequate record keeping, corporate action errors					
Risk from external events through operational failure at suppliers or out sourced operations, fire or natural disaster, Terrorism, Vandalism, pilferage, theft and robbery etc					

12. Does Standard Chartered bank carryout suspicious transaction monitoring on customer's accounts?

- i).Yes ii) No

13. If yes, who is responsible for the monitoring?

- i). Tellers
- ii) .Supervisors
- iii). Managers
- iv).General Managers
- v).Others, specify-----

14. How often is suspicious transaction monitoring carried out on the customer accounts?

- i).Daily
- ii).Once a quarter
- iii).Once every 6 months
- iv).Once a year
- v).Others (specify) -----

15. In transaction monitoring, how crucial are the following factors in respect to customer suspicious transactions?

	Very crucial	Crucial	Fairy crucial	Hardly crucial	Not crucial
Verification of Sources of large customer deposits					
Review of the customer account transaction history					
Verification of customers against the list of blacklisted individuals					
Know your customer campaigns during the account opening exercise					

8. Have there been cases of fraud in Standard Chartered bank?

- i) Yes
- ii) No

a) If yes, what are some of cases in your institution?

- i) Suppression of customer deposits
- ii) Forgery of customer signatures
- iii) Manipulation of customer cash deposit slips
- iv) Others, please specify _____

b) How were these cases of fraud detected?

- i) Whistle blowing hotline
- ii) Internal tip off
- iii) By accident
- iv) Internal audit
- v) External tip off
- vi) Others factors, please specify-----

9. What are the major causes of fraud in your organisation?

- i) Poor internal controls
- ii) Insufficient staff training
- iii) System failures
- iv) Collusion by members of staff
- v) Poor staff motivation
- vi) Others, specify-----

10) What are some of the warning signs (red flags) that may signal fraud by an employee in your institution? (Select any option where appropriate)

- i) Reluctance to take leave
- ii) Refusal of promotion
- iii) Sudden change of lifestyle
- iv) Cosy relationship with suppliers/ contractors
- v) First to arrive in the morning and last to leave at night
- vi) Others specify-----

SECTION C: The role of operational risk management in combating fraud

1) Are there programs/ procedures that aim at creating operational risk awareness in combating fraud in your institution?

- i) Yes
- ii) No

If yes, please answer the questions below;

- 2) What are these programs
- i) Operational procedures
 - ii) Training activities/ awareness programs
 - iii) Workshops/ Seminars
 - iv) Others, please specify _____

3) How are these programs conducted in your institution?

- i) Seminars and workshops
- ii) Sharing personal experiences among members of staff
- iii) Emphasis on the best practices
- iv) Openness among employees
- v) Others, please specify _____

4) Have these programs had an impact in combating fraud in your institution?

- a) Yes
- b) No

5) If yes, what impact have the programs created in combating fraud in your institution?

- Fraud cases have reduced to a minimal level
- i) Customers have gained confidence in the Institution
- ii) The institution commands a higher reputation from the public

- iii) Perpetrators of fraud can be easily identified by the employees
- iv) Employees have become more vigilant while handling any customers
- v) Suspicious transactions can easily be identified
- vi) Others, please specify _____

SECTION D: Creative measures of operational risk management in combating fraud to an acceptable level

1) Do you have a fraud prevention plan in your organisation?

- i) Yes
- ii) No

If yes, how important is the following in mitigating the risk of fraud in your organisation

	Very important	important	Fairly important	Not important
Introduction of an ethics policy statement				
Introduction of a fraud policy statement				
Establishment of a control environment and operational control procedures				
Introduction of a fraud education, training and awareness programs				
Constant review of all anti-fraud policies and procedures				
Introduction of a whistle blowing policy				

2) Does your organisation take any action once fraud by a member of staff/ customer has been detected?

- a) Yes
- b) No

If yes, what actions are taken?

- i) Ignored
- ii) Reported to supervisors
- iii) Investigated further
- iv) Identification of perpetrators

v) Black listed

vi) Others, specify -----

3) What measures are taken by your organisation upon discovering a member of staff involved in fraud?

i) Dismissal

ii) Further investigation

iii) Counselling

iv) Others specify-----

SECTION E: The relationship between operational risk management and fraud

1) The following is important in operational risk management and fraud

	Strongly Agree	Agree	Disagree	Strongly Disagree
Operational risk awareness minimises fraud in organisation				
Fraud detection starts with operational risk assessment				
System failures increase the risk of fraud in an organisation				
Internal control failures can facilitate fraud in an organisation				
Fraud education, training and awareness programs minimise the risk of losses from fraudulent activities				

2) Does your operational/ risk manual guide in the management of the risk of fraud?

a) Yes

b) No

Give reasons for your answers_____

SECTION F: Give any other opinions about operational risk management and fraud

In your opinion

1) Why is fraud persistent in the banking institutions today?-----

2) What measures must be put in place to combat e fraudulent activities in the banking institutions?-----

Thank you for your time and cooperation