OPERATIONAL RISK MANAGEMENT AND FINANCIAL FRAUD MANAGEMENT IN TELECOMMUNICATION COMPANIES: A STUDY OF AIRTEL UGANDA

BY

MICHAEL LUKYAMUZI

REG: 11/MMSFM/26/018

A DISSERTATION SUBMITTED TO THE HIGHER DEGREES DEPARTMENTS IN PARTIAL FULFILLMENT OF REQUIREMENTS FOR THE AWARD OF MASTER'S DEGREE IN MANAGEMENT STUDIES (FINANCIAL MANAGEMENT) OF UGANDA MANAGEMENT INSTITUTE

NOVEMBER, 2013

DECLARATION

I, **Michael Lukyamuzi** hereby declare that this dissertation is my original work and has never been submitted for any academic award or publication in any institution or University. Due acknowledgement has been made for the work of others in this report, through quotation and references.

Signed _____

Michael Lukyamuzi

Date_____

APPROVAL

This is to certify that this dissertation entitled "OPERATIONAL RISK MANAGEMENT AND FINANCIAL FRAUD MANAGEMENT IN TELECOMMUNICATION COMPANIES: A STUDY OF AIRTEL UGANDA" was conducted under our supervision.

_____

DR. MARY BASAASA MUHENDA

Date: _____

_____

DR. MARIA K. BARIFAIJO

Date: _____

DEDICATION

This work is dedicated to my dear Mother Rose Kakumba for her unswerving support towards my success, thank you Mum.

ACKNOWLEDGEMENT

I would like to express my thanks and gratitude to various people who contributed to the completion of this work. It is not possible to name all those who supported me but I am greatly indebted to everyone. I wish to express my sincere gratitude to my supervisors Dr. Mary Basaasa Muhenda and Dr. Maria K. Barifaijo whose support, guidance and constructive criticism and their untold commitment to supervise this research.

I extend special thanks to the management and staff of Airtel Uganda for accepting to respond to this study with commitment.

CONTENTS

LIST OF FIGURE

LIST OF TABLES

LIST OF ABBREVIATIONS

ACFE	:	Association of Certified Fraud Examiners
COSO	:	Committee of Sponsoring Organizations Framework
CVI	:	Content Validity Index
ORM	:	Operations Risk Management
RMT	:	Risk Management Training

ABSTRACT

The study is on the relationship between operational risk management and financial fraud management in telecommunication companies with particular emphasis on Airtel Uganda. Specifically the study investigated the relationship between training of personnel, internal systems, company processes and financial fraud management in Airtel Uganda. The study used a cross sectional design adopting both quantitative and qualitative approaches using a sample of 148 respondents consisting of Heads of department and sections, Senior Managers, supervisors and team contributors. Data was collected using a questionnaire and interview guide. The study found a high positive significant relationship between personnel, internal systems, company processes and financial fraud management in Airtel Uganda. The study concluded that conducting of operational risk focusing on identification of employee training needs and development of employee knowledge and skills significantly influences financial fraud management in telecommunication companies. The study concluded that conducting of operation risk focusing on network connectivity, access logs, records management and maintenance significantly influences financial fraud management. The study concluded that conducting of operational risk focusing on company processes of segregation of duties, supervision and reconciliations significantly influences financial fraud management. The study recommends that to achieve the desired level of financial data integrity, financial fraud reporting and mitigation of financial loss, the management of telecommunication companies should continuously identify ORM annual training needs at the individual level without compromise of the departmental and unit levels, strengthening of access logs and trails, and effective supervision of management actions by the company board.

CHAPTER ONE

INTRODUCTION

1.0 Introduction

The research investigated the relationship between operational risk management and financial fraud management in the telecommunication companies, a case study of Airtel Uganda Limited. This chapter covers the background to the study, the statement of the problem, the purpose of the study, the research questions, the hypotheses, the scope of the study, the significance, justification and operational definition of terms and concepts.

1.1 Background to the Study

The Background is based on four perspectives that is; historical perspective, theoretical perspective, conceptual perspective and contextual perspective.

1.1.1. Historical Background

Risk-taking is an inherent trait of any enterprise. There can be no growth or creation of value in a company without risk-taking. However, if risks are not properly managed and controlled, they can affect the company's ability to attain its objectives, therefore risk management and internal control systems play a key role in directing and guiding the company's various activities by continually preventing and managing risks (Leitch, 2008). The need to manage risk has arisen in many fields and the telecommunication sector is no exception to this trend and the approaches used in each reflect the skills and interests of the people involved and the availability of relevant data. The objective of risk management is, to maximize the productive efficiency of the enterprise. One can

imagine a proto-risk manager burning a fire at night to keep wild animals away (Peter, 1996). Early lenders must have quickly learned to reduce the risk of loan defaults by limiting the amount loaned to any one individual and by restricting loans to those considered most likely to repay them. Individuals and firms could manage the risk of fire through the choice of building materials and safety practices, or after the introduction of fire insurance in 1667, by shifting it to an insurer. However, it wasn't until the 1960s that the field was formally named, principles developed and guidelines established. Mehr & Hedges (1960) widely acclaimed as the fathers of risk management, enumerated the following steps for risk management process: identifying loss exposures; measuring loss exposures; evaluating the different methods for handling risk; risk assumption; risk transfer; risk reduction; selecting a method and monitoring results (D'Archy, 2001).

In the present business environment, Mishra and Prasad (2006) noted that financial fraud has enormous consequences for the victim telecom company, its employees, creditors, investors, and for society at large. It may lead to reduced salaries and benefits for the organization's employees, the loss of jobs or job opportunities, investment losses, lower sales volume due to an organization's tarnished reputation, an increase in sales prices, change of ownership, bankruptcy or even the liquidation of assets. Payne and Gainey, (2004) also noted that occupational fraud may also generate other indirect costs for employees and investors in the victim organization, such as pain and suffering, mental health treatment and a lower quality of life.

According to ACFE and Peltier-Rivest (2007) noted that the failure to prevent and detect fraud has serious consequences for organizations. In the USA, it is estimated that the financial costs associated with employee fraud is around fifty billion dollars ($50 billion) annually (Coffin, 2003). A recent survey in the UK indicates that the cost of employee fraud to listed companies alone

amounts to some two billion pounds (£2 billion) a year (Management Issues News, 2005). In 2004, an Australian and New Zealand KPMG study of four hundred ninety one (491) large businesses showed that twenty seven thousand six hundred and fifty seven (27,657) incidents of fraud occurred in the two years from April 2002 to March 2004, with total losses amounting to $456.7 million (KPMG Forensic, 2004). The study also revealed a diverse set of fraudulent activities including financial statement fraud, misappropriation of assets, information theft and receipt of kickbacks or bribery. Further, the major perpetrators of fraud were found to be employees, and almost Sixty seven per cent (67%) of such fraud was committed by those at management level.

The Association of Certified Fraud Examiners (ACFE, 2010) fraud report covered one thousand eight hundred forty three (1,843) occupational fraud cases in more than one hundred countries (100). Of these cases, approximately ninety percent (90%) involved asset misappropriations. From the cases studied, the ACFE estimated that the typical organization loses five percent (5%) of their annual revenue to fraud which the ACFE estimate that this five percent (5%) figure would translate to approximately $2.9 trillion as applied to the estimated 2009 Gross World Product.

According to Li & Nadeem, (2010) efficiently managing operational risk in telecommunication companies is critical for the survival and growth in the economic globalization waves. He continues to say that many large companies that filed for bankruptcy protection were mainly due to poor operational risk management and failure to manage financial fraud like embezzlement of cash, falsification of accounts, factious transactions and forgery during the last two decades.

The evidence on the prevalence of fraud and its perpetrators as indicated in the contemporary literature acknowledges the prevalence of corporate financial fraud in developed countries with sophisticated fraud management systems and agencies. It leaves to question the extent to which

ORM influences financial fraud management in the telecommunication industry in developing countries.

1.1.2. Theoretical Background

In recent years the topic of risk management has moved up the agenda of both government and industry, and private sector initiatives to improve risk and fraud management systems have been mirrored by similar promptings for change in the public sector. Both regulators and practitioners now view operational risk management as an integral part of the process of corporate governance, and an aid to the achievement of strategic objectives (Woods, 2008). This study was underpinned by the contingency theory as advanced by Fielder (1964) which states that there is no best way to organize a corporation, to lead a company or to make decisions. Instead, the optimal course of action is dependent upon the internal and external situation.

Contingency theory has sought to formulate broad generalizations about the formal structures that are typically associated with the use of different technologies. The perspective originated with the work of Joan Woodward (1958), who argued that technologies directly determine differences in such organizational attributes as span of control, centralization of authority, and the formalization of rules and procedures. Some important contingencies for companies are; technology, suppliers and distributors, consumer interest groups, customers and competitors, government and unions (Woodward, 1958).

Contingency model focused on a contingency model of leadership in organizations. This model contains the relationship between leadership style and the favorableness of the situation (Fielder, 1964). Situational favorableness was described by Fiedler in terms of three empirically derived dimensions; the leader-member relationship, which is the most important variable in determining

the situation's favorableness, the degree of task structure, which is the second most important input into the favorableness of the situation, the leader's position power obtained through formal authority, which is the third most important dimension of the situation. Situations are favorable to the leader if all three of these dimensions are high. That is, if the leader is generally accepted and respected by followers that is the first dimension, if the task is very structured that is the second dimension, and if a great deal of authority and power are formally attributed to the leader's position which is the third dimension, then the situation is favorable.

The contingency theory is further supplemented with the Vroom and Yetton's decision participation contingency theory or the normative decision theory. According to this model, the effectiveness of a decision procedure depends upon a number of aspects of the situation: the importance of the decision quality and acceptance; the amount of relevant information possessed by the leader and subordinates; the likelihood that subordinates will accept an autocratic decision or cooperate in trying to make a good decision if allowed to participate; the amount of disagreement among subordinates with respect to their preferred alternatives (Vroom & Yetton, 1973). And today risk management is a very important area in the Telecommunication Sector.

All telecom companies strive to manage their risks if they are to prosper and continue operating in the challenging market. Managing risk is very vital for corporations; Airtel Uganda is continuously coming up with new products to delight their customers as they strive to be the most preferred and affordable brand in the daily lives of Africans by 2015.To decide on whether to avoid, mitigate, reduce or accept an operational risk necessitates making a decision by company management as whether to take on an opportunity as many opportunities have many probable risks that have to be put into consideration.

1.1.3. Conceptual Background

Risk is inherent in every economic activity and every organization has to manage it according to its size and nature of operation because without risk management no organization can survive in the long run (Dorfman, 2007). This is because businesses today are faced with far greater challenges than before due to the fact that economical, technological and legal interdependence are becoming more prevalent and pronounced. It would be assumed that operational risk management and financial fraud management systems will vary from organization to organization based on their size or industry sector. It is therefore logical to assume that every business organization has put in place a strong operational risk management structure and financial fraud management systems to help achieve its goals. These are fundamental to the successful operation and day-to-day running of a business and assist a company in achieving its objectives (Gleim, 2008).

Operational risk management focuses on adopting a systematic and consistent approach to manage all the risks confronting an organization in terms of the personnel, systems and processes. With the emergence of the world as the global village, companies are diversifying their activities in order to remain competitive for example Telecommunication companies taking on the business of value added services like transferring money, thus resulting in increased risks.

Besides the core business activities, the increased use of derivative products by both financial and non-financial Institutions and recent events of scandals continue to demonstrate the need for enhanced standards and processes of control over risk that is the segregation of duties, supervision and reconciliations. Control environment is one of the five components of the internal control

systems and it is the foundation of all other five components providing discipline and structure (Gleim, 2008).

Risk management framework issued by the Committee of Sponsoring Organization of the Treadway Commission ('COSO') report defines internal control as a process designed to provide reasonable assurance regarding the achievement of objectives in relation to effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations.

1.1.4. Contextual Background

The Government of Uganda adopted a four-part strategy to facilitate the rapid expansion of the telecommunications sector to introduce competition in the industry. This included the licensing of the first mobile operator, Celtel (1993), and the second national telecom operator, MTN Uganda Limited, in April 1998. The introduction of competition into the sector occurred as early as September 1993 when Clovergem Celtel Ltd was licensed to provide nationwide mobile telephony services. This was later followed by the opening up the value added services market which resulted in issuance of various licenses in 1995 and 1996 for paging services, satellite services (private voice and data services), VSAT services, public pay telephone, mobile trunked radio services, and customer premises internal block wiring services. The company has taken a rebranding journey from Celtel to Zain and of recent to Airtel. The management is responsible for ensuring that there is an effective, integrated operational risk management framework. This should incorporate a clearly defined organizational structure with defined roles and responsibilities for all aspects of operational risk management, monitoring and appropriate tools that support the identification, assessment, control and reporting of key risks. All this has been put in place but the company

continues to lose revenues in system and people errors, fraud and inefficiency. In the month of August a revenue gap of up to forty thousand dollars ($40,000) was discovered on the roaming platform. In Airtel Uganda a fraud amounting to approximately twenty nine million five hundred seventy nine and eight hundred shillings (UGX 29,579,800) was detected in October 2011 in the One Stop Shop (Njoroge, Tay, & Ruhui, 2012). The country has seen so many Telecom Companies lose money in frauds, fail to break even (Marchetti, 2012). Very little is known about operational risk management and financial fraud management in the telecom sector, it is for this reason that the researcher is interested in examining it.

1.2 Statement of the Problem

Operational Risk Management aspects of personnel training, instituting of internal organizational system and processes are undertaken by every organization envisaging effective fraud management (Collier et al., 2007; Gleim, 2008; Lieberum, 2004& Subramaniam, 2008). Despite the efforts to undertake employee training in ORM, network connectivity, secured controlled access logs, records management, segregation of duties, supervision and performance of periodic reconciliations in mobile telecommunication firms, the telecommunication industry in Uganda has experienced huge irrecoverable financial scam. In the month of May 2012, a fifteen billion shillings (Ugx 15 Billion) mobile money fraud was reported in one of the big Telecom Company's mobile money which had been going on for 2-3years (Mbanga, 2012; Tushabe, 2012). This is not an isolate case as it was reported that an accountant had been arrested in a Telecom fraud case where police queried how very large sums of money had gone unaccounted for at the company without reporting and escalation for such a long time (John, 2012). If this trend was to continue without management interventions in the ORM practices, telecommunication customers would lose confidence in the industry yet the communication commission may council the operating

license of affected telecommunication companies for failure to effectively manage financial fraud. It is against this background that the study investigated telecommunication's operational risk management and its effect on financial fraud management.

1.3 Purpose of the study

The study intended to empirically study the relationship between operational risk management and financial fraud management in telecommunication companies with particular emphasis on Airtel Uganda

1.4 Objectives of the study

1. To investigate the relationship between training of personnel and financial fraud management in the Telecommunication Companies.
2. To investigate the relationship between company internal systems and financial fraud management in Telecommunication Companies.
3. To investigate the relationship between company processes and financial fraud management in Telecommunication companies.

1.5 Research Questions

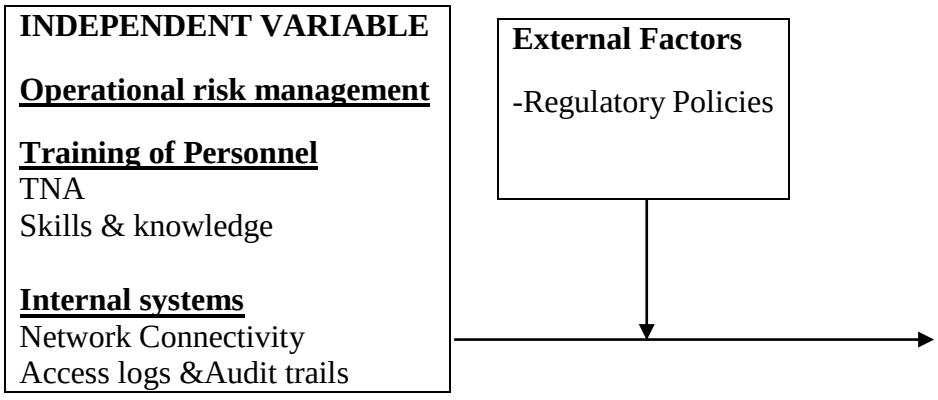
1. What is the relationship between training of personnel and financial fraud management in the Telecommunication Companies?
2. What is the relationship between company internal systems and financial fraud management in Telecommunication Companies?
3. What is the relationship between company processes and financial fraud management in Telecommunication companies?

1.6 Hypothesis of the Study

1. There is a significant relationship between training of personnel and financial fraud management in the Telecommunication Companies.
2. There is a significant relationship between company internal systems and financial fraud management in Telecommunication Companies.
3. There is a significant relationship between company processes and financial fraud management in the telecommunication companies.

1.7 Conceptual Framework

The conceptual framework below will be the guiding factor of the study to assess the relationship between operational risk management and financial fraud management in telecommunication companies. Figure1: shows the conceptual framework components of operational risk management (IV) and financial fraud (DV). The Operational risk management is conceptualized as training of personnel, internal systems and processes while financial fraud management is conceptualized as embezzlement of cash, falsification of accounts, fictitious transactions, revenue loss.



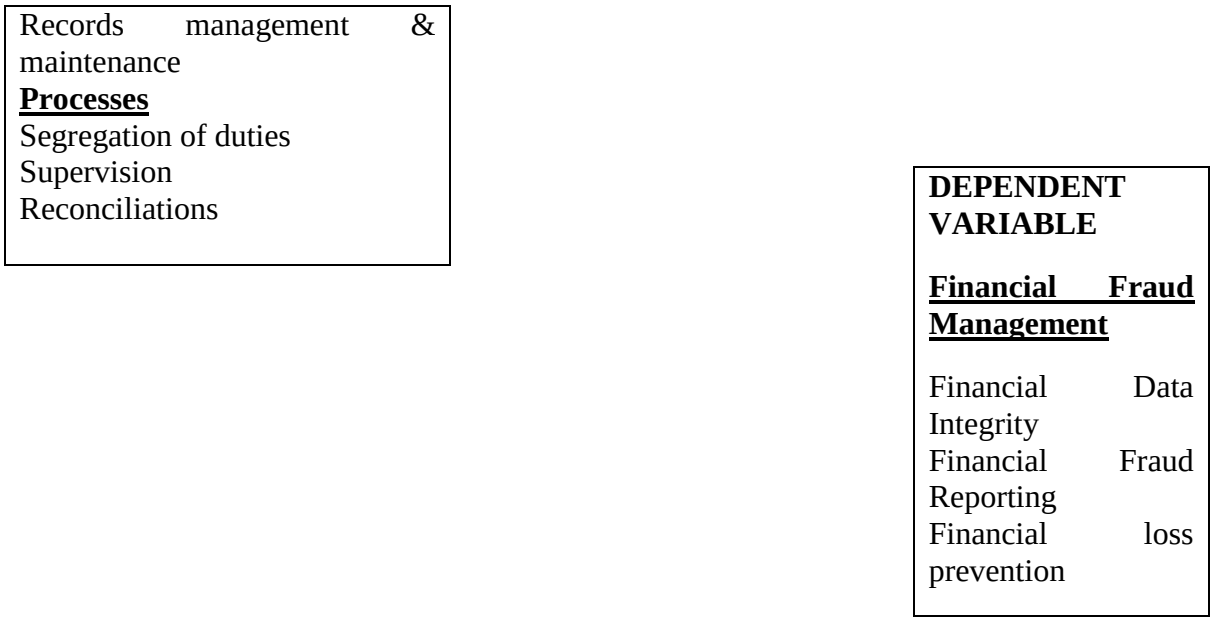


Figure1: Conceptual framework

Source: Adopted from the Committee of Sponsoring Organizations Framework (COSO, 1992); and Morells Internal Control Systems Model, (2008).

The conceptual framework above hypotheses a relationship between operational risk management and financial fraud, it anticipates that personnel, internal systems and processes have a strong relationship with financial fraud management for example the skills and knowledge possessed by the company personnel will enable them to identify the possible areas of revenue leakage and close them.

1.8 Significance of the study

This study may be useful in the following ways:

To the Board and management of Telecommunication companies, the study helps develop empirical evidence for strengthening ORM policies for enhanced fraud management to protect the hard earned revenue of the company.

To the academia, the study helps fill literature gaps on the relationship between ORM practices of personnel training, internal systems, organizational processes and fraud management in the telecommunication sector.

1.9 Justification of the study

Several years ago the telecoms industry began to realize that, typically, 2 - 5% of revenue was not even billed due to a combination of system problems and mistakes. Sometimes the loss was over 10% of revenues. This money is lost profit. Initial disbelief turned to acceptance as people realized the many ways in which occasional errors combined and accumulated to big money (Leitch, 2004). With the knowledge of the ever amassed revenue loss and leakages, there is an increasing need to assess the impact of operational risk management on financial fraud management in telecommunication companies. This thesis will focus on the relevance of operational risk management that will include but not limited to the personnel, processes, internal systems and external event and there contribution to financial fraud management. The study is the first of its kind in the company and will therefore provide first hand practical experience on operational risk management and financial fraud management within the telecom industry.

1.10 Scope of the Study

1.10.1 Content scope

This study focused on the operational risk management practices like training of personnel, internal systems and processes and their relationship with financial fraud management.

1.10.2 Geographical scope

This study was conducted at the Airtel Uganda head office at Airtel house in Kampala Uganda, it is believed to represent all the characteristics under study as the biggest part of the Airtel team sits at the head office.

1.11 Time scope

The study focused on the time scale from November 2010; the time scale is justified by the fact that Airtel Uganda kick started its operations in Uganda in the same year.

1.12 Operational Definitions

Internal Control is the process and the system that ensures the optimum utilization of resources to meet goals and objectives, as well as safeguard assets. Internal control is not merely an accounting function; rather it links with the whole organization. Internal control; Promotes operational efficiency and effective utilization; Provides reliable and relevant information; Safeguards assets and records; Ensures adherence to laid out policies and ensures compliance with statutory requirements (Panwar, 2009).

Internal Control System consists of rules, procedures and organizational structures - designed to pursue values of substantial and procedural fairness, transparency and accountability, which are considered fundamental to the business of Telecoms, as established by the company's code of ethics and conduct (Telecom Italia , 2011).

Operational Risk management (ORM) Under Basel II developed by the Bank for International Settlements (BIS) 2, operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." The definition explicitly includes legal risk, but excludes strategic and reputation risk.

Risk identification is a process designed to identify first both the strategic objectives and goals and then the potential internal and external events that can adversely affect the enterprise's ability to achieve those objectives and goals (Marchetti, 2012).

Fraud according to Pagare (2000) and Manasse (2004), fraud means deception, cunning or trickery or acts committed by a person with an intention to deceive or cheat others. This is a definition adopted by this study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter is based on ideas generated by other scholars which are related to the research topic at hand. Mugenda & Mugenda (1999) asserts that reviewing of literature involves the existence and thorough systematic identification, location and analysis of documents containing information related to the research problem being investigated. The first section presents the theoretical review. This is followed by a review of related literature on ORM dimensions of training of personnel, internal systems, company processes and fraud management.

2.2 Theoretical Review

In order to make a decision on the course of action to implement for the probable risks, management has to make a decision (Leitch, 2008). In this study the contingency theory was analyzed to ascertain its compatibility to address the need to make a decision. Basically, contingency theory asserts that when managers make a decision, they must take into account all aspects of the current situation and act on those aspects that are key to the situation at hand (Vroom & Yetton, 1973).

Contingency theory has sought to formulate broad generalizations about the formal structures that are typically associated with or best fit the use of different technologies. The perspective originated with the work of Joan Woodward (1958), who argued that technologies directly determine differences in such organizational attributes as span of control, centralization of authority, and the

formalization of rules and procedures One example of an integrated solution to risk management is enterprise risk management" (CIMA, 2005).

The Institute of Risk Management also provided a more detailed definition of risk management as: the processes by which organizations methodologically address the risks to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. In 1992, COSO issued the internal control – integrated framework with the intention of helping businesses and other entities assess and enhance their internal control systems and control their activities toward the achievement of their established objectives. It however became clear that there is the need for a stronger framework to effectively identify, assess and manage risks. This does not however replace the internal control framework, but rather incorporates the internal control framework within it and telecom companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process (COSO,2004).

Steiburg & Tanki, (2005) while quoting from the COSO Report of September 1992, defined ICS as a process effected by an entity's board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of objectives in the following categories; effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations. These authors went on to state that COSO report provides a comprehensive and a common definition of ICS that serves the need of all users. For the purpose of this study, the internal control system means all the systems, people, policies, procedures, and practices that are in an organization to ensure that operational risk is managed, mitigated and avoided, orderly and efficient conduct of the business, adherence to the applicable laws and the accuracy and completeness of the accounting records.

The importance of the ICS stemmed from the fact that no firm, large or small, is exempted from the danger of Fraud (Lieberum, 2004). The author went on to say that one way of avoiding operational risk or closing a gap is by instituting internal controls into the telecom firm's culture. Woolf, (1997) and Gupta & Arora (2004) agreed with this assertion, and stated that ICS should be established in any organization in order to avoid revenue leakages and operational risk, among other things. It means that detection and prevention of operational risk becomes an important role of the internal control system (ICS). Other objectives for establishing the ICS include: to carry on the business of the organization in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets, secure as far as possible the completeness and accuracy of the records and timely preparation of reliable financial information.

The above is further supported by Arens & Loebbecke (1997) who observed that physical assets of an organization can be stolen, misused or accidentally destroyed unless they are protected by adequate controls. To the researcher, these objectives of establishing the ICS do equally apply to the Telecom Companies, particularly that of detecting and preventing operational risk.

2.3 Operational Risk Management and financial fraud management

The management of risks is very important and significant to the achievement of business objectives and therefore plays a key role in a telecom company's system of financial fraud management and corporate governance. Leitch, (2004) published an article on Risk Management versus Internal Control. In this article, he noted that there is no difference between these two topics in principle. He went on to point out that the scope of each phrase seems to be getting wider. However, there are big differences in emphasis, with many practical implications. In the researcher's opinion, the management of risks and their control measures are inseparable. First,

risks must be identified, assessed, then managed and mitigated by putting in place or implementing a strong system of internal control. As a result of separation of ownership from control, both the corporate world and governments turn to risk management and internal controls to give calm and reassurance (Collier et al., 2007).

Poupart (2010) noted that risk management and internal control systems complement each other in controlling the telecom company's activities. The risk management system aims to identify and analyze the company's main risks. Risks that exceed the acceptable levels set by the company are dealt with and, as the case may be, subject to plans of action. These plans may call for the implementation of controls, a transfer of the financial consequences (through insurance or an equivalent mechanism) or an adaptation of the organizational structure. The controls to be implemented are part of the internal control system. In this way the internal control system contributes to the management of the risks incurred in the telecommunication company's activities. The internal control system relies on the risk management system to identify the main risks that need to be controlled. In addition, the risk management system needs to include controls that are part of the internal control system and aimed at ensuring the proper functioning of the risk management system.

Telecom Companies use internal control mechanisms to ensure that staff respects their organizational policies and procedures. However, internal control alone cannot ensure that the Telecoms adequately minimize its risk exposures. Only if the Telecom Company's risk management strategies are effectively integrated into its policies and procedures can the internal control function support risk minimization (Campion, 2000). For example, a Telecom Company experiencing increasing arrears in it postpaid services might decide to reduce its exposure to credit risks, by developing stricter lending credit terms or limiting increases in unpaid arrears. The

Telecom Company links internal control to risk management by creating mechanisms to evaluate the results of these delinquency reduction efforts, such as by requiring the Finance team to regularly monitor the customer's credit worthy.

According to Campion (2000) internal control and internal audit play important roles in the risk management feedback loop, in which the information generated in the internal control process is reported back to the Board and management. Internal control mechanisms work to improve decision making by ensuring that information is accurate, complete and timely so that the board and management can respond to control issues promptly as they arise. In addition, if the telecom Company links its financial risk management mechanisms to operational risk management, the instituted financial fraud management controls can identify remaining risk exposures and inform management.

Operational risk management actions are supported by policies and procedures that, when carried out properly and in a timely manner, manage or reduce financial losses as a result of no reconciliations (COSO, 2006). In the same way that managers are primarily responsible for identifying the financial and compliance risks for their operations, they also have line responsibility for designing, implementing or monitoring their financial fraud management control system (Arens & Loebbecke, 1997; Hael, 1999).

Vanasco (1998) emphasized that fraudulent financial statements were a great concern to the corporate world and the accounting profession and explained the ideal control environment to prevent fraud and also focused on the techniques and preventive procedures in the investigative and reporting process. In addition, the writer elaborated on white-collar crimes constituting employee fraud, embezzlement, kiting, larceny, lapping and pilferage. This study specifically

developed literature themes on training of personnel, internal systems, company processes and their influence on financial fraud management.

2.3.1 Training of personnel and financial fraud management

A telecommunication company's control environment can be seriously eroded if a significant number of positions are filled with persons lacking required job skills (Comision, 2003). He continues to say that managers will encounter the situation from time to time when a person has been assigned to a particular job but does not seem to have the appropriate skills, training, or intelligence to perform that job. Lieberum, (2004) supplements that all humans have different levels of skills and abilities thus adequate supervision and training should be available to help employees until proper skills are acquired. He continues to say that a telecom company needs to specify the required competence levels for its various job tasks and to translate those requirements into necessary levels of knowledge and skill. He adds that by placing the proper people in appropriate jobs and giving adequate training when required, an enterprise is making a commitment to competence, an important element in the organization's overall control environment and financial fraud management.

Apostolou (2000) examines the knowledge considerations of persons conducting financial fraud review and states that to conduct a fraud examination, the persons required skills to properly detect and investigate an allegation of fraud and also knowledge of the legal elements and which law to apply. The need for knowledge in legal elements of fraud is informative and helped develop insight into the need to assess the possession of legal knowledge in the telecommunication industry by the staff conducting operations risk at the different levels in the company.

Comision (2003), Apostolou (2000) and Lieberum, (2004) assertions on the need to consider personnel skills and capacities in placement of employees in the different functional units of the firm although widely acknowledged, it does not offer the competence profile for necessary for effective ORM in the telecommunication sector. This study has however filled this literature gap of which it has found out that it was necessary for telecommunication sector employees to possess skills related to establishing risk indicators, capturing risk data at their level, risk management procedures, applicable regulations, accounting, communication and IT skills.

Leitch (2008) argues that managers often find it valuable to assess whether adequate position descriptions have been created, whether procedures are in operation to place appropriate people in those positions, and whether training and supervision are adequate. Poupart (2010) affirms this by saying that management in each entity ensures that the company's operational risk management policy is applied. He adds that management is responsible for applying this policy and ensure that exposure to these risks complies with the executive management's risk management policy. He continues to say that all employees concerned should possess the knowledge and information required for creating, operating and monitoring risk management and financial fraud in light of the objectives assigned to them. This is particularly true of line managers dealing directly with the risk management and internal control systems, as well as with the internal controllers who manage the resources of the company (Poupart, 2010).

However there is no guarantee that identifying risk will enable the implementation of effective and efficient controls on financial fraud. Why? Because knowing the potential operational risk does not prevent collusion between two or more people who are in positions to circumvent the internal control mechanisms or prevent managers or individuals in key leadership capacities from unduly influencing those responsible for internal control activities. Therefore it is important for staff to

recognize the ignored controls and report to the appropriate authority (Worrells, 2008). In support of the above,

The COSO (2004) framework asserts that Enterprise risk management is a process designed to identify potential events that may affect the entity, and to manage risks within the entity's risk appetite so as to provide reasonable assurance regarding the achievement of entity objectives. The COSO (2004) framework therefore posits that Risk Management Training (RMT) is therefore important and it is expected that when managers are more aware of the various business risks facing their organization, they are more likely to ensure that risk management training is actively undertaken for staff members, and this is expected to lead to improved internal control quality. In support, Farrugia (2002) asserts that staff training is a key element in risk management and one that needs constant reappraisal with regard to the type of risk and design of controls as organizations operate in a dynamic environment.

In line with the above Kramer (2003) argued that employees who are actively trained in risk management are likely to more accurately identify threats to the organization as a result of weak or non-existent internal controls. Further, with risk management training, staffs are also likely to appreciate the linkages of risks across different sections of the firm and the implications of internal control breakdowns from a firm-wide perspective. Consequently, such staff may be expected to not only develop a more compliant attitude to following set rules and procedures, but also may even suggest viable improvements to procedures, which will ultimately improve internal controls. The above authors' views and opinions on risk management training and the related outcomes of enhancing trainee attitudes to conducting of risk management in the firm needed to be examined in a telecommunication context to help fill literature gaps and generalization of risk management training and specifically to operational management training. This study correlation results

revealed that training of personnel which facilitates the gaining of the desired skills had high positive significant relationship with financial fraud management in the telecommunication sector of Uganda.

2.3.2 Internal Systems and Financial Fraud Management

Operational systems set the tone of a telecom company, influencing the control consciousness of its people, it is the foundation of all the other components of operational risk management providing discipline and structure (Stienhoff, 2001). Warrels (2008) puts it:

No matter how complex the structure, if it doesn't have a solid foundation, its integrity will be unreliable. The foundation of a control system on financial fraud management is the philosophy of business and people controlling the business. Before distinguishing the controls one must consider the foundation.

Arens and Loebbecke (1997) asserts that in practice, the board of directors is informed of the key characteristics of the financial fraud and risk management systems chosen and implemented by executive management: organizational structure, roles and functions of the main players, procedures, risk reporting and control system monitoring structure. More specifically, the Board checks with executive management to ensure that the monitoring, internal control and risk management systems are adequate to ensure the reliability of the company's financial reporting and to provide a fair view of the company's and the group's earnings and financial situations. The Board may use its general powers as needed to have any audits or verifications that it deems timely carried out or to take any other action that it deems appropriate in this regard (ibid). The literature as highlighted by the above authors focused on the role of board of directors in exercising an

oversight role in risk management but offers no specific mechanism that the board of a telecommunication board of directors could adopt on overseeing risk management in the firm.

A telecom company internal process related to sharing of where pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information that makes it possible to run and control the business (Stock, 1999). Although the Stock (1999) identifies internal communications systems as necessary for carrying out their responsibilities, the piece of work seems anecdotal as it offered no details on how information could be shared in operational risk management context. This created a knowledge gap on how best organizations could effectively manage their information sharing for effective performance of the different roles in the telecommunication sector of a developing country.

McNamee (1999) introduced risk assessment as a tool to help to detect and deal with fraud in operations of organizations. He emphasized that managers had to take responsibilities to locate fraud. Risk assessment could also be used as a decision-making tool to assist managers sort through a number of possibilities and single out those with the greatest payoff. Furthermore, managers could use this technique to identify and prioritize the most likely business processes where potential fraud could occur. McNamee further analyzed the three elements of risk assessment were risk identification to determine the high-risk areas and its sources while risk measurement to determine the consequences of the risk and likelihood of its occurrence. Risk prioritization is to determine the appropriate resources to manage the risk.

Colbert and Alderman (1995) introduced the approaches adopted by auditors in deriving an audit strategy. The two approaches were procedures-driven approach and the risk-driven approach. Procedures-driven approach did not make full consideration of the risk present. In this approach, the auditor determined the specific audit procedures to be performed without considering the objective of the related risk.

The internal audit function has gained an expanded role in corporate governance (Gramling, 2004) and now involves the provision of additional services initiated by the board of directors or the audit committee (Christopher et al., 2009). In a US survey study, the chief audit executives of many organizations reported the detection of fraud through the internal audit function (Campbell and Lindsay, 1994). The effectiveness of this function may be attributable to the reasonable use of and compliance with internal auditing standards (Leung &Cooper, 2009; Abdolmohammadi, 2009). Research has also shown that an effective internal audit function can provide advance notice of fraud risk, thereby helping to detect and prevent fraudulent financial reporting (Gramling & Myers, 2003).

Rae and Subramaniam (2008) observed that besides, auditing financial transactions, IA activities may also cover non-financial areas such as business unit processes, geographical areas and compliance with laws and regulations. Case study observations by Peterson and Gibson (2003) found that IAs' recommendations for improving ICP are critical for not only preventing control breakdowns but also for detecting fraud as well. In this study, it is argued that the more extensive an IA function, the greater the likelihood that weaknesses in ICP are identified. Consequently, through better identification of ICP weaknesses, appropriate remedial measures may then be undertaken, leading to a higher quality ICP. The literature on the role of IA in improving on ICP was generic and merely anticipated relationships as it provided no imperial evidence. This study

therefore strived to cover this literature gap by establishing the IA activities in the telecommunications sector.

Crawford and Weirich (2011) noted that corporate counsel may be in a key position to review information indicating the existence of asset misappropriation by employees and is quite likely to be the recipient of tips by employees, customers or vendors. The ACFE (2010) report indicated that such tips accounted for approximately 40 percent of all frauds detected. By contrast, only 4.6 percent of the frauds were detected by external audits. Setting up an anonymous tip reporting mechanism and enforcing rigorous background checks on new employees in responsible management and financial positions are generally recognized as two antifraud measures that have a noticeable impact on the size of losses incurred. The corporate counsel can be most effective in an antifraud program by looking for financial reporting that does not square with their understanding of the economic realities of the business, looking for situations where the form of a transaction differs from the substance and carefully reading the critical financial reports prepared for the public, shareholders and lenders.

Although the available literature generally hints on the role of internal audits and corporate councils in mitigating financial fraud, it failed to highlight how internal processes of network connectivity, access logs and audit trails, records management and maintenance influence financial fraud management in the telecommunication industry. This study has helped cover this knowledge gap by observing that internal systems were the single highest predictor of the variance in financial fraud management in the telecommunication firm under study.

2.3.3 Processes and financial fraud management

Steinburg and Tanki (2005) defined operational risk management as the policies and procedures put in place to ensure that management directions are carried out. They help ensure the necessary actions by management are taken to address risks in order to achieve the objectives of the organization, such as detecting and preventing financial fraud (ishungwa, 2001). Such activities permeate the entire organization. These activities include; authorization and approval, arithmetical and accounting procedures, segregation of duties, chart of accounts, system manuals, physical controls and independence checks (Arens & Loebbecke 1997, Steinberg & Tanki 2005).

According to Comision (2003) management ensures where practicable, policy formulation, supervisory and other internal process review or advisory functions, including where applicable compliance and internal audit, are effectively segregated from line operational duties. Such segregation serves to ensure the effectiveness of supervisory and other controls on financial fraud management established by management. Stock, (1999) supplements that the responsibilities of both directors and management are well defined in the operational risk management policy where reviewing the effectiveness of internal control on financial fraud is an essential part of the Board's responsibilities while management is accountable to the board for developing, operating and monitoring the system of internal control and for providing assurance to the board that it has done so.

It was in this study's best interest to establish how the internal systems of segregation of duties was undertaken in the telecommunication sector of Uganda of which it was found that segregation of duties was not adequately undertaken which constrained effective fraud management in the telecommunication firm under study.

Ashbaugh-Skaife, Kinney & LaFond (2006) argue that firms with operational risk management deficiencies have higher idiosyncratic risk. The higher the idiosyncratic risk, the more likely a firm will experience a large drop in reputation, which typically triggers shareholder class-action lawsuits. This suggests that firms with financial fraud control weaknesses have additional exposure to litigation and operational risk, and are more likely to inflict damages to their auditors' reputation.

Campion (2000) noted that when assessing the need for processes and procedures, the Board should consider whether it has other means of obtaining sufficient and objective assurance regarding the effectiveness of the system of the processes. The Board should also have regard to any trends or current factors in the company's internal environment, markets or other aspects of its external environment that may have increased, or be expected to increase, the risks faced by the company. Worrells (2008) says that in the absence of an explicit operational risk management process, the personnel manager is initially not conscious or aware of the risks to which she is exposed and the potential opportunities available. The literature seems to explore the different efforts to exercise supervisions in the firm but it was not elaborate on how best to implement supervision in the telecommunication sector which is highly automated and electronic. This study however found out that supervision was at its lowest and it constrained effective fraud management a finding which has helped contribute to body of knowledge on the role of supervision in effective financial fraud management

Differences in fraud loss amounts may result from variations in the degree of authority and financial control exercised at different job levels. For example, managers, top executives and owners have greater access to company funds, assets, and confidential information than lower level employees (Wells, 2008; KPMG, 2009). Within organizations, the hierarchical position may either

limit or facilitate certain types of fraud (Holtfreter, 2005). Executives and owners may also have more authority to override existing controls than lower level employees, thus allowing the fraud to grow and go undetected for a longer period of time than other frauds (ACFE, 2008; KPMG, 2009).

Collusion involves any kind of explicit or implicit agreement between two or more persons to perpetrate a fraud, whether the accomplice is internal or external to the victim organization. The organization's internal controls may fail because of collusion among employees (COSO, 1992, 2004). Collusion often allows employees to circumvent controls that would otherwise detect the fraud earlier and limit its impact (ACFE, 2008).

Segregation of duties is an important control to prevent and detect fraud. When people collude to override these controls, segregation of duties becomes ineffective and fraud is more likely to go undetected for a longer period of time (KPMG, 2009). Peltier-Rivest and Lanoue (2012) study concluded that designing and implementing controls which mitigate the risk of collusion to reduce the increased losses that normally result from such frauds is essential for organizations. Simple controls, such as segregation of duties and anonymous reporting hotlines, may very well prevent and detect large frauds before financial damages irrevocably harm the organization.

Bowe and Jobome (2001) discussed the designation of a managerial framework to control the operational risk, and focus on unauthorized trading fraud. A sample of 37 cases was taken for examination from financial institutions in eight countries over the period 1984-1999. The sample results indicated that internal controls were the primary defence against severe fraud losses and showed that the regulatory penalties imposed on senior supervisory management, in addition to the fraudster, were crucial in ensuring efficient mitigation of fraud loss. Losses from unauthorized

trading fraud can be identified with breakdown of controls and constraints designed to mitigate losses from operational risk. However, Seetharaman et al., (2004) crirtises this paper by noting that only one type of fraud was analyzed, as there may be other types of fraudulent activities in the financial services industry. The survey also failed to identify the motives of fraud and other preventive measures to combat fraud.

To Commercial Angles' Newsletter (2001c), the best way of preventing fraud was to understand why it happened. Fraudsters generally identify an opportunity for exploiting a weakness in the control procedures and then assess whether their potential rewards would outweigh the penalties should they be caught. In addition, the paper introduced the two-stage processes of fraud prevention. First, an organization must ensure that opportunities for fraud were minimized: fraud prevention. Second, organization should ensure that potential fraudsters believe they will be caught: fraud deterrence. Introduction and enforcement of new controls would reduce the opportunities for perpetrators. A regular control was most effective and normally required little management time or effort. It also emphasized the importance of having strong management and a healthy corporate culture to detect and consequently deter fraud. The limitation of this paper is that it did not specify the detailed control procedures for two-step processes of fraud prevention. It failed to explain the financial effects and risk of computer fraud if prevention and deterrence procedures were not in place. This study strived to fill this literature gap by providing empirical evidence how ORM challenges constrains the effective management of financial fraud in the telecommunications industry.

Seetharaman et al., (2004) contends that preventing fraud consists of those actions taken to discourage the perpetration of fraud and limit the exposure if fraud does occur. Nobody can guarantee that fraud will not occur. Given its inherent limitations, even an effective internal control

structure cannot provide more than reasonable assurance that fraud will be prevented. Nevertheless, by initiating adequate internal controls by management, good employment practices and training programs, organizations can take a proactive stance in warding off fraud and keep losses to minimum.

Numerous anecdotal evidence indicates that internal control procedures (ICPs) are an important element in preventing and detecting fraud. Peterson and Gibson (2003) detail a case where poor ICP procedures relating to a lack of segregation of duties and absence of an independent reconciliation of cash and poor documentation were seen as factors that enabled fraud to occur. For instance, the senior cashier who was caught embezzling was found to have responsibility over both the recording and the custody of cash. Similarly, other studies also demonstrate that the absence of segregation of duties by combining incompatible roles and control breakdowns have been instrumental in enabling fraud to be committed (Buckhoff, 2002; MacArthur et al., 2004).

Graham et al. (2005) surveyed over 400 US financial executives and found disturbingly that poorly performing firms are likely to take measures to delay bad news, that reported earnings rather than cash flows are the major metric analyzed by stakeholders, meeting or exceeding benchmarks is very important to executives' credibility, executives prefer smooth rather than volatile earnings, and that they feel pressure to take decisions that may sacrifice long-term value to meet earnings targets. Mechanisms used to meet benchmarks would include a range of accounting discretionary choice such as changing in accounting assumptions together with discretionary spending choices such as deferral of investment projects.

Financial fraud management mechanisms that are efficient and effective cannot be identified and implemented unless the operational risks faced have been identified. According to Leslie (1984)

and Millichamp (1998), segregation of duties is one of the prime means of operational risk management that if combined would reduce risks of intentional manipulation or error and increase the element of checking. Segregation has to be combined with reconciliation and supervision as Opondo (2006) emphasizes that a good starting point for effective and efficient internal controls and fraud prevention which is an integral part of operational risk management and internal controls system is for top management to develop a code of conduct that re-enforces the culture of compliance and accountability.

The literature although elaborate on the need to segregate responsibility, effectively supervises and performs reconciliation; it did not provide evidence on the extent to which these forms of organizational processes could have contributed to effective fraud management. This study has held cover this knowledge gap by establishing a positive significant relationship between organizational processes and financial fraud management.

2.4 Summary of Literature Review

The literature provided an insight on the influence of training of personnel and fraud management but fell short of providing empirical evidence on the relationship between operational risk management aspect of personnel training and financial risk management in the telecommunications sector. This study strived to cover this literature gap by examining the relationship between operational risk management, training needs analysis and knowledge and skills possessed by the personnel and their contribution to financial fraud management in the telecommunication industry. Similarly, the literature did not provide information on how an internal systems of network availability, access logs, and records management contributes to financial fraud management. This study therefore helped cover this literature gap by providing empirical evidence that there was a high significant relationship between internal systems of

network availability, access logs, and records management and financial fraud management in the telecommunication industry. Last but not least, the literature did not provide evidence on the relationship between ORM practices related to separation of duties, supervision and reconciliations and financial fraud management. This study has helped cover this literature gap by providing evidence that there is a significant relationship between ORM processes and financial fraud management in the telecommunication sector of Uganda.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter presents the study design, study population, sample size, sampling design, data collection methods, instruments, validity and reliability, research procedure, data analysis and measurement of variables.

3.2 Research design

A cross sectional survey descriptive design combined with both qualitative and quantitative approaches will be used. As justified by Amin (2005), a correlation design was also used in the study since it describes in quantitative terms the degree to which variables are related. It involves collecting data to determine whether and to which degree a relationship exists between the two variables under study. Pearson's Correlation coefficient was used to express the degree of the relationship.

3.3 Study population

Amin (2005) defines a population as a complete collection of all elements that are of interest in a particular investigation. The study population comprised of one hundred and forty eight respondents (148) distributed across all the eleven of the company Departments, the eleven Departments that included; mobile commerce, finance, information technology, human resource, supply chain management, marketing, sales and distribution, networks, customer service, managing director's office as they are the are all relevant to the study and they are directly involved

in financial fraud management and operational risk management. The composition of the intended study population is indicated in Table 1.1.

3.4 Determination of the Sampling size

The study sample size indicated in Table 1 below and the determination criterion was adopted from Krejcie & Morgan, (1970) sample size table. Using this study the sample size for all Departments was based on their population size.

Category Of Respondents	Population	Sample Size	Sampling Technique
Team Contributors	170	100	Random Sampling
Supervisors, Managers & Team Leaders	25	15	Random Sampling
Senior Managers and Section Heads	45	27	Random Sampling
Heads of Department	11	6	Purposive Sampling
Total Airtel Employees	251	148	

Airtel, (2011) Talent Acquisition and Talent Management Report Financial Year April 2011 – March 2012

The table above highlights the departments that were included in the study, the size of the population in each department, the sampling technique that was administered as well as the justification for the technique adopted.

3.5 Sampling techniques and procedure

Doscombe, (2000) asserts that a sample needs to be carefully selected if there is to be confidence that the findings from the sample are similar to those found among the rest of the category under

investigation. Probabilistic and non-probabilistic sampling techniques were used, the target population was divided into different stratum based on Departments and a list of staff with in the selected departments shown in Table 1.1 to act as the sample frame per stratum. With probabilistic sampling, each member's name was written on a paper and the researcher employed the Gold Kish method under simple random sampling to single out the final respondents and these were administered with questionnaires. The non-probabilistic sampling was use in form key informant respondents who were purposively selected comprising of departmental heads, management, finance team and supervisors who are directly involved in the implementation of the operational risk management policy and data from this group was collected using interview guide.

3.6 Data Collection Methods

The researcher used tools that were deemed relevant by using both primary sources of data from questionnaires and interviews of the selected population and secondary sources of data was literature already reviewed and collected by scholars on operational risk management like journals, text books, magazines, internet, and reports.

3.6.1 Survey Questionnaires

The study used as self-administered questionnaire. This tool for data collection was used because respondents can easily express themselves with no interference from the researcher. As justified by Amin (2005), a questionnaire is a carefully designed instrument for collecting data in accordance with the specifications of the research questions and hypotheses.

3.6.2 Interviews

These were conducted by the researcher through the purposive sampling strategy as guided by Marjorie (2003). Marjorie asserts that in every community, family, neighborhood, workplace and schools, there are people who have knowledge and skills to share. The study specifically interviewed the compliance manager and internal controller.

3.7 Data collection instruments

Data from the field was obtained using a combination of data collection instruments like questionnaires that was self-administered with the dichotomous questions, objectives questions and a few open ended and structured question and interview guide to select information from the finance director, revenue assurance and fraud manager, compliance manager, finance controller, internal controller and revenue assurance analysts, finance manager, line managers and departmental heads and it was guided by the interview guide that has simple questions, non-structured questions developed by the researcher and administered to the subject of the study.

3.7.1 Questionnaire

As justified by Amin (2005), a questionnaire is a carefully designed instrument for collecting data in accordance with the specifications of the research questions and hypotheses. The study used a close ended questionnaire divided into sections of background information, ORM and fraud management. A standard Questionnaire on a five point Likert scale was used to get quantifiable primary data from individual respondents. The scale was designed as indicated below: 1- Strongly Disagree; 2- Disagree; 3- Not sure; 4- Agree; 5- Strongly Agree.

3.7.2 Interview Guide

The interview guide was developed by the researcher to be used when conducting interviews for the purposive sampling strategy as guided by Marjorie (2003). Marjorie asserts that in every community, family, neighborhood, workplace and schools, there are people who have knowledge and skills to share. The interview focused on a set of semi-structured questions focusing on ORM aspects of training of personnel, internal systems and company processes.

3.8 Quality Control Instrument

To ensure quality data in terms of reliability and validity, a quality control assessment was carried out.

3.8.1 Validity

Validity according to Wangusa (2007) is the extent to which the instrument measures what it was supposed to measure, in other words it is the researcher's process of ensuring that any measuring instrument selected measures what it purports to measure or portrays the truth in the findings that are consistent with the desired objective or theory. The study used a content validity index (CVI) based on expert judgment taking only variables scoring above 0.70 accepted for social sciences (Amin, 2005) using the formula:

$$CVI = \frac{\text{Number of item declare valid}}{\text{Total Number of items}}$$

Table 2: Content Validity Results

Variable	Total No of items	Number of valid items	CVI
Training of personnel	13	11	0.85
Internal systems	12	10	0.83
Processes	12	11	0.92
Financial fraud management	15	13	0.87

Source: Expert Judgment

Table 3 shows that training of personnel yielded CVI of 0.85, internal systems yielded a CVI of 0.83, company processes yielded a CVI of 0.92, while financial fraud management yielded a CVI of 0.87. Since all variables yielded a CVI above 0.70 accepted for social sciences, it was inferred that the instrument was relevant in measuring ORM and financial fraud measurement.

3.8.2 Reliability

Reliability measures the degree to which a research instrument yields consistent results or data after repeated trials (Mugenda & Mugenda, 2003). The reliability of a measure indicates the extent to which it is without bias and hence ensures consistency measurement across time and across the various items in the instrument (Sekaran, 20003). In this study a Cronbach's alpha coefficient was computed to show how reliable the data is using Software Package for Social Sciences (SPSS) and the results are presented below.

Table 3: Reliability Results

Variable	Total No of items	Reliability
Training of personnel	13	0.851
Internal systems	12	0.798
Processes	12	0.850
Financial fraud management	15	0.894

Source: Primary data

Table 3 above shows that training of personnel yield Cronbach's alpha value of 0.851, internal systems yielded alpha value of 0.798; processes yielded alpha value of 0.850 while financial fraud management yielded alpha value of 0.894. Since all variables yielded an alpha value higher than 0.70 accepted for social sciences, it was concluded that the instrument was consistent in measuring ORM and financial fraud management and therefore reliable.

3.9 Procedures for data collection

Prior to data collection undertaking in the field, an introduction was sought from Uganda Management Institute and accessibility granted at Airtel Uganda Management. The research instruments were formatted in consistence with the research themes, objectives and questions. Primary data was derived from individual response through interviews.

3.10 Data analysis

The data was analyzed through both qualitative and quantitative analysis

3.10.1 Qualitative Analysis

For qualitative analysis, the researcher organized statements, and responses to generate useful conclusions and interpretations on the research objectives (Sekaran, 2003). Qualitative analysis involved coding of data, identifying categories and patterns that emerge and reporting them in narrative form using themes (Mugenda & Mugenda, 1999) on the study variables of training of personnel, internal systems and company processes.

3.10.2 Quantitative Analysis

Quantitative data was presented in form of descriptive statistics using frequency and percentages. Mean and standard deviations for each of the variables were also used in the study. A mean result ranging from 1-1.49 was considered as strongly disagree, 1.50-2.49 was considered as disagree while a mean in the range of 2.5.-3.49 was considered as not sure. A mean in the range of 3.5-4.49 was considered as agree while a mean in the range of 4.5-5 was considered as strongly agree.

Pearson's coefficient r and significance p tested at the 95 and 99% confidence limits were used to test if there was any significant relationship between the independent and dependent variable. A positive correlation coefficient r indicates a direct positive relationship between the variables while a negative correlation indicates an inverse, negative relationship between the two variables (Amin, 2005).

The regression analysis was used to test the extent to which the independent variables predicted the variance in the dependent variable using ANOVA statistics of adjusted R^2 values, beta, t values and significance values (Amin, 2005). Specifically the adjusted R^2 value gave a statistical indicator

of the percentage to which the independent variable predicted the variance in the dependent variable. All these were generated from the primary data set programmed in SPSS.

CHAPTER FOUR

PRESENTATION, ANALYSIS AND INTERPRETATION OF RESULTS

4.1 Introduction

This chapter presents analyses and interprets the study findings on operational risk management and financial fraud management in Airtel Uganda. The first section presents the response rate, this is followed by the background information about the respondents, presentation and analysis of the study findings in relation to the specific objectives.

4.2 Response rate

A total of one hundred forty eight (148) questionnaires were distributed but one hundred sixteen (116) useable questionnaires were returned giving a response rate of seventy eight percent (78%) which was high. Amin (2005) suggested that a response rate of forty percent (40%) and above is a reasonable representation of the study sample selected from the population.

4.3 Background information

This section gives the characteristics of the respondents in relation to their education, time worked and job title in Airtel Uganda. This is based on the information provided on the questionnaire by the respondents themselves in the study questionnaire.

Table 4: Background information about the respondents used in the study

Item	Description	Frequency	Percentage
Education level	Diploma	2	1.7
	Degree	58	50.0
	Postgraduate	42	36.2
	Professional	14	12.1
	Total	**116**	**100.0**
Time worked	Below 5 years	81	69.8
	5-10 years	31	26.7
	10-15 years	2	1.7
	15 years and above	2	1.7
	Total	**116**	**100.0**
Job title	Head of Department	6	5.2
	Senior manager	19	16.4
	Manager	42	36.2
	Supervisor	21	18.1
	Regional sales team leader	3	2.6
	Team contributor	25	21.6
	Total	**116**	**100.0**

Source: Primary data

Table 4 above shows that majority of 50% of the respondents had attained a university degree as their highest level of education followed by 36.2% who had attained a Postgraduate qualification and 12.1% who had professional qualifications such as ACCA, CPA, CIMA and the like as their highest level of education. This finding suggested that the respondents had attained a reasonable level of education to be trainable operational risk management and to effectively manage risk at their level and mitigate financial fraud in Airtel Uganda.

In relation to time worked, the majority of 69.8% of the respondents had worked for less than 5 years while 26.7% had worked with the company for 5- 10 years. The least number of respondents (1.7%) each had worked with the company for 10-15 years and more. This was the case as the company had just undergone acquisitions in 2010 whereby new structures were created with new personnel hired. Never the less, these findings suggested that most staff will need continuous

training to enhance their competencies in operational risk management since the majority had not been in the company for a reasonable time.

4.4 Training of Personnel and Financial Fraud Management

The first objective of the study was to investigate the relationship between training of personnel and financial fraud management in the Telecommunication Companies. Training of personnel was one of the dimensions of operational risk management and had two indicators of training needs assessment, knowledge and skills measured using 13 items scored on five (5) point Likert scale ranging from 1= Strongly Disagree (SDA), 2 = Disagree (DA), 3 = not sure (NS), 4= Agree (A), 1= Strongly Agree (SA) and the findings are shown in table 5 below using Mean and Standard Deviation (SD).

Table 5: Descriptive Statistics for Personnel Training

Personnel Training	**Percentage (%)**				**Mean**	**S.D**
	SDA	**DA**	**A**	**SA**		
Training Needs Assessment						
Airtel undertook to identify your operations risk management training needs necessary in the telecommunication sector of Uganda	51.7	30.2	18.1	00	1.84	1.11
The identified operational risk training needs contribute to the existence of the company	6	00	50.9	31.9	4.09	0.82
The identified operational risk training needs are relevant for the achievement of the objectives of your department	00	3.4	48.3	36.2	4.17	0.77
The identified operational risk training needs are relevant to your roles and responsibilities in the company	00	9.5	43.1	38.8	4.11	.92
Knowledge and skills						
You possess the necessary knowledge in capturing risk data at your level	2.6	6	49.1	30.2	3.98	0.95
You possess the necessary knowledge in risk control assessment	2.6	9.2	48.3	19	3.72	0.97
You possess the necessary knowledge in establishing indicators of key risks to the company operations at your level	2.6	12.1	56.9	20.7	3.81	0.99
You possess knowledge of telecommunication operations risk procedures	39.7	38.8	21.6	00	2.03	1.13
You possess knowledge of telecommunication operations risk applicable regulations	36.2	40.5	19.8	00	2.07	1.10
You possess adequate accounting knowledge	44.8	31.9	23.3	00	2.02	1.12
You have the ability to validate proper data for a specific risk analysis	41.4	33.6	25	00	2.05	1.15
You are capable of communicating operational risk recommendations at you level	41.4	38.8	19.8	00	1.98	1.10
You possess strong IT skills necessary to conduct operational risk analysis in the telecommunications sector	43.1	35.3	19.8	00	1.79	1.12
Average Mean					**2.90**	**1.02**

Source: Primary data

The results in table 5 above revealed an aggregated mean of 2.90 which implied that the respondents agreed and as well as disagreed with the majority of the items of personnel training in ORM. The Standard deviation ranged between 0.92 and 1.15, which was relatively narrow suggesting that most means did not deviate from the central mean by a big margin.

Item 3 which asked whether the identified operational risk training needs were relevant for the achievement of the objectives of the employee's department received the highest mean of 4.17

suggesting that ORM training needs assessment emphasized departmental risk management needs. However item 13 which asked whether the respondent possessed strong IT skills necessary to conduct operational risk analysis in the telecommunications sector and item received the lowest mean of 1.79 suggesting that most employees did not possess adequate IT skills necessary for effective management of operational risk at their level which reduces their effectiveness in ensuring financial data integrity, financial reporting and financial loss prevention.

In the next subsection an item by item analysis is provided on each of the indicators of planning management functions of environmental analysis, schedule development and resource planning.

4.4.1. Training Needs Assessment

Table 5 shows that majority of 82.8% of the respondents agreed (mean = 4.09) that the identified operational risk training needs contributed to the existence of the company while 84.5% agreed (mean = 4.17) that the training needs were relevant for the achievement of the objectives of the department. A total of 81.9% agreed (mean = 4.11) that the training needs were relevant to their roles and responsibilities in the company. However, 81.9% the respondents disagreed (mean = 1.84) that Airtel undertook to identify their operations risk management training needs necessary in the telecommunication sector of Uganda. These findings suggested, operational risk management training needs assessment focused on existence of the company, were based on the departmental needs and employee responsibilities which should be commended as it helps contribute to identification of training gaps necessary for effective management of risk at the functional level. However, the failure to identify individual training needs compromises the effectiveness of the consequential operational risk management training interventions due to a perceived personal irrelevance of the training. It was therefore necessary that the operational risk

management company, departmental, team and individual level training needs are continuously identified in unison to make the ORM training relevant at all levels.

Asked to describe the ORM training needs assessment practices in Airtel, interviewee I put it:

"The training needs assessment in Airtel is done at the Unit level with the Unit heads that is to say if the new staff is under Revenue assurance, the operational risk management training needs assessment is done with the manager revenue assurance and so on".

Interviewee II had this to say;

"The TNA is carried out with the unit heads and job description of the particular staff. As the staff continues in the role, weak areas are identified and he or she is helped or guided by the unit manager to improve on performance".

The interview findings suggested that training needs are carried out generally as a routine for human resource training but not specifically for ORM training gaps. Thus the inclusions of ORM training needs at each individual officer levels rests on its inclusion in the annual training needs identification.

4.4.2 Knowledge and Skills

Table 5 above shows that a majority of 79.3% of the respondents agreed (Mean = 3.98) that they possessed the necessary knowledge in capturing risk data at their level, while 78.6% agreed (mean = 3.81) that they possessed the necessary knowledge in establishing indicators of key risks to the company operations at their level. A majority of 67.3% agreed (mean = 3.72) that they possessed the necessary knowledge in risk control assessment. These findings suggested that about eight (8) in every ten (10) staff had the desired knowledge in capturing risk data and establishing indicators

for the identified risk which contributes to effective financial fraud management. However 2 in every10 employees did not possess knowledge in capturing risk data and establishing risk indicators which may affect their effectiveness in identifying and mitigating financial fraud at their level.

On the contrary, a majority of 77.5% of the respondents disagreed (mean = 2.03) that they possessed knowledge of telecommunication operations risk procedures while another 76.7% disagreed (mean = 2.07) that they possessed knowledge of telecommunication operations risk applicable regulations. A total of 80.2% disagreed (mean = 1.98) that they were capable of communicating operational risk recommendations at their level while 78.4% disagreed (mean = 1.79) that they did not possess strong IT skills necessary to conduct operational risk analysis in the telecommunications sector. These findings suggested that 8 in every 10 staff in Airtel did not possess adequate knowledge of telecommunication operations risk procedures, applicable regulations, communicating operational risk recommendations and did not possess strong IT skills necessary to conduct operational risk analysis in the telecommunications sector which incapacitates them to adequately identify and mitigate financial fraud at their levels. It was necessary that the management of the company improves on these critical ORM knowledge and skills gaps for effective fraud management.

Asked to describe how staff competence in conducting ORM at their levels, interviewee replied:

Very competent as the escalation criteria is very clear with higher risks or those that cannot be resolved escalated for higher guidance. However there is a challenge of specialization of staff in particular competences like in the IT platform and sales with people ignoring hygiene issues and dependences like areas of revenue leakage. Many times the staff in areas of IT, Sales and

Marketing ignore controls in their roles for example the marketing teams always want to push through new products without taking time to identify the possible flaws.

Interviewee I responses seem to agree with interviewee II response who had this to say:

The staff are well trained and experienced staff are usually recruited, many of the current crop of Airtel staff were outsourced from other organizations, and with this the company is sure of competent staff in performing their roles. The challenge is that is there are limited knowledgeable and experienced resources in the ORM for all the Telecom companies. The available resources are usually obtained from the banks, many of which lack the technical understanding of the Telecom infrastructure and operation.

The above interview findings agree with the quantitative findings in that they agree that most staff possessed the desired competencies in conducting ORM at their level which should ideally lead to enhanced fraud mitigation if they had the right attitudes and if the skills are put into practice. There is however, limited supply of specialized personnel in the telecoms ORM prompting a need to develop such ORM skills profession in the telecommunications industry.

4.4.3. Correlation analysis between personnel training and financial fraud management

To test the relationship between personnel training and financial fraud management Pearson's correlation analysis was conducted at the 2-tailed level and the findings are presented below.

Table 6: Correlation matrix between training of personnel and financial fraud management

Variable		1	2
Training of Personnel	Pearson Correlation	1	
	Sig. (2-tailed)		
Financial Fraud Management	Pearson Correlation	.545**	1
	Sig. (2-tailed)	.000	
**. Correlation is significant at the 0.01 level (2-tailed).			

$P \leq 0.05$

Table 6 above shows Pearson's correlation coefficient r = 0.545** and p = 0.000 between training of personnel and financial fraud management suggesting that there was high positive significant relationship between personnel training and financial fraud management. The implication was that effective financial fraud management in Airtel depends on the efforts to identify employee training needs, developing their knowledge and skills in operational risk management. The study therefore qualified the hypothesis that there is a significant relationship between training of personnel and financial fraud management in the Telecommunication Companies. The study findings on the relationship between training of personnel and financial fraud management calls for the management of telecommunication firms to adequately consider the identification of operational risk Management training needs and equipping the staff with the necessary skills, knowledge and attitudes to effectively perform operational risk management activities.

Asked to describe how personnel training affect financial fraud management in Airtel, one interviewee put it:

"Personnel training empowers staff to identify assess and monitor frauds in their particular roles"

Another interviewee has this to say:

"Training improves the vigilance of staff while performing their roles. The personnel will be cautious of the flaws in the performance of their roles, will easily accept and appreciate the implemented controls in the management of revenue leakages".

The interview findings seem to agree with quantitative findings that training of personnel was vital as it enabled employees gain the skills and knowledge necessary to perform their duties with competence.

4.5. Internal systems and Financial Fraud Management

The second objective of the study was to investigate the relationship between company internal systems and financial fraud management in the Telecommunication Companies. Company internal system was one of the dimensions of ORM and had three indicators of network connectivity, access logs and audit trails, records management and maintenance measured using 12 items scored on five (5) point Likert scale ranging from 1= Strongly Disagree (SDA), 2 = Disagree (DA), 3 = not sure (NS), 4= Agree (A), 1= Strongly Agree (SA) and the findings are shown in table 7 below using Mean and Standard Deviation (SD).

Table 7: Descriptive Results for Internal System

Internal Systems	Percentage				Mean	S.D
	SDA	DA	A	SA		
Network connectivity						
The Airtel network connectivity is always reliable in ensuring transactional data quality	2.6	12.1	41.4	21.6	3.67	1.03
There are adequate alternatives to access transactional data in the event of network interruptions	1.7	11.2	39.7	24.1	3.73	1.01
The network has clear data recovery mechanisms for the vital customer account information like account balance, account profile.	2.6	12.1	24.1	21.6	3.66	1.03
There are adequate data backups to provide transactional data in the event of loss of a data source	1.7	9.5	21.6	41.6	3.80	0.99
Access logs and trails						
There is an internal system which allows you to easily access the relevant chronological transactional records as documentary evidence for a specific operation		16.4	37.1	28.4	3.78	1.04
Access to the transaction records is authenticated		5.2	40.5	31.9	3.99	0.87
The internal system in Airtel provides for segregation of roles of all actions by users	46.6	35.3	18.1		1.90	1.09
Audit trails of transactions performed by a user are protected from manipulation by other users	49.1	26.7	18.1		1.93	1.13
Records management and Maintenance						
The internal system creates adequate records that you can use to audit transactions at your level	62.9	14.7	16.4	2.6	1.81	1.24
The internal system can store adequate records that you can use to audit transactions at your level	50	28.4	18.1		1.90	1.12
The internal system provides for adequate records security	44.8	25	21.6	2.6	2.12	1.27
The internal system can adequately retrieve records necessary for risk analysis	38.8	28.4	21.6	2.6	2.21	1.24
Aggregated mean					**2.43**	**1.14**

Source: Primary data

The results in table 7 above revealed an aggregated mean of 2.43 which implied that the respondents disagreed with the majority of the items of company internal systems in ORM. The Standard deviation ranged between 0.87 and 1.27, which was relatively narrow suggesting that most means did not deviate from the central mean by a big margin.

Item 6 which asked whether the access to the transaction records was authenticated received the highest mean of 3.99 suggesting that authentication of users to access transaction records was an emphasized to help track users actions and accountability for their actions. However item 9 which asked whether the internal system created adequate records that one could use to audit transactions

at their level received the lowest mean of 1.81 suggesting that user were constrained by inadequate records management system necessary to effectively audit transactions at their level which reduces their effectiveness in identifying and mitigating financial fraud.

In the next subsection an item by item analysis is provided on each of the indicators of planning management functions of environmental analysis, schedule development and resource planning.

4.5.1 Network Connectivity

Table 7 above shows that majority of 63% of the respondents agreed (mean =3.67) that the Airtel network connectivity was always reliable in ensuring transactional data quality, while another majority of 63.8% agreed (mean = 3.73) that there were adequate alternatives to access transactional data in the event of network interruptions. A total of 45.7% of the respondents agreed (mean = 3.66) that the network had clear data recovery mechanisms for the vital customer account information like account balance, account profile while majority of 63.2% agreed (mean = 3.80) that there was an adequate data backups to provide transactional data in the event of loss of a data source. These findings suggested that the reliable network, availability of alternative to access data in the event of network break down and data recovery mechanism enhances the effectiveness of the ORM system as it helps in guaranteeing availability of raw data for interrogation.

Asked to describe how Network Connectivity affects ORM, interviewee I put it that:

"Network connectivity is the gateway to the system, if it is well managed that is through restricted entry and penetration of the system frauds can be deterred".

Interviewee II had this say on network connectivity:

"The Telecom business is run on an infrastructure that is involves connection of various nodes and there is a lot to lose like revenues, customer information, and reference data in case of network disconnection".

The above indicates that network connectivity is crucial for the management of the operational risk in the telecommunication industry. This is so because with the availability of the network any anomalies happening like unauthorised access of the network, modification and manipulation of records will be captured and arrested accordingly.

4.5.2. Access logs and trails

Table 7 above shows that majority of 65.5% of the respondents agreed (mean = 3.78) that there was an internal system which allowed them to easily access the relevant chronological transactional records as documentary evidence for a specific operation while 82.4% agreed (mean = 3.99) that access to the transaction records was authenticated findings which suggested that efforts was undertaken to manage access to chronological transactional records and authentication of access to data which enhances data security management and mitigation of financial fraud through the minimized risk.

However, 81.9% of the respondents disagreed that the internal system in Airtel provided for segregation of roles of all actions by users (mean = 1.90) while 75.8% disagreed (mean = 1.93) that Audit trails of transactions performed by a user were protected from manipulation by other users. These findings suggested that weakness in the security of the access logs and audit trails as users were not only well segregated by their actions, but were also not protected from manipulation by other users after executing their transactions which implied high rate of system based investigation leakages which may lead to financial loss. It was therefore necessary that the management of the company undertakes immediate action to segregate actions and protect users from the manipulation of transactions to mitigate financial loss by the users in its ORM practices.

Asked to describe how Access logs affects ORM, interviewee I put it that:

"It is the access logs and audit trails which are used for transaction monitoring and tracking. Logs and trails are used for investigation of frauds, confirming and assurance that there are no revenue leakages through undercharging customer transactions"

Interviewee II had this to say:

"The Access logs are for monitoring and ensuring that the right people with the right privileges access the system which creates and enables and audit trail in case of any suspicious transactions or anomalies occurring".

It was observed that all activities on the telecommunication network are captured which allows auditing for assurance and certainty that the acceptable activities are all that run on the network.

4.5.2 Records management and Maintenance

Table 7 above shows that majority of 77.6% of the respondents disagreed (mean = 1.81) that internal system created adequate records that could be used to audit transactions at their level while another 78.4% disagreed (mean = 1.90) disagreed that the internal system could store adequate records that they could use to audit transactions at their level. Similarly, a majority of 69.8% of the respondents disagreed (mean = 2.12) that the internal system provided for adequate records security while 67.2% disagreed (mean = 2.21) that the internal system could adequately retrieve records necessary for risk analysis. The failure by the system to adequately create, store and secure records necessary for effective audit, suggested material weaknesses in the internal records management and maintenance leading to failure to adduce the necessary transactional evidence in the ORM leading to financial loss. The management needs to take action by developing a responsive, sound and parallel records management and maintenance system for effective management of financial fraud.

Asked to describe how records management and maintenance affects ORM, interviewee I had this to say:

"The records management is for accountability and tracking. It is a regulatory requirement, the maintained records are used for internal and external audits, and they are used for tax audits to".

Interviewee II was brief and said:

"Records management and maintenance allows availability of information as and when it is needed".

4.5.4. Correlation analysis between Company Internal Systems and Financial Fraud Management

To test the relationship between company internal systems and financial fraud management Pearson's correlation analysis was conducted at the 2-tailed level and the findings are presented below.

Table 8: Correlation matrix between company internal systems and financial fraud management

Variable		**1**	**2**
Internal Systems	Pearson Correlation	1	
	Sig. (2-tailed)		
Financial Fraud Management	Pearson Correlation	844.**	1
	Sig. (2-tailed)	.000	
**. Correlation is significant at the 0.01 level (2-tailed).			

$P \leq 0.05$

Table 8 above shows Pearson's correlation coefficient r = 0.844** and p = 0.000 between company internal systems and financial fraud management suggesting that there was high positive significant relationship between company internal systems and financial fraud management. The implication was that effective financial fraud management in Airtel depends on company internal systems related to network connectivity, access logs and audit trails, records management and

maintenance. The study therefore qualified the hypothesis that there is a significant relationship between company internal systems and financial fraud management in the Telecommunication Companies. Thus when network connectivity is guaranteed 24/7, every minute and every second, it guarantees the availability and quality of transactional data on the system which enables the execution of ORM activities at the different levels which contributes to an efficient financial fraud management system. Similarly, access log controls help in the controlling and tracking of responsibility in the event of transactional data manipulation while records management ensures that there is a permanent point of reference to back up documentary evidence of a transaction which contribute to an efficient financial fraud management mechanism in the telecommunication company.

Asked to explain the company internal systems affect financial fraud management in Airtel one interviewee had this to say:

"Enforce that the right personnel are accessing the system that is to say the persons with the right privileges and in the right role. Transactions are monitored to ensure correct charging for transaction that is without any under or over charging"

4.6. Company processes and Financial Fraud Management

The third objective of the study was to investigate the relationship between company processes and financial fraud management in the Telecommunication Companies. Company processes was one of the dimensions of ORM and had three indicators of segregation of duties, supervision and

reconciliations measured using 12 items scored on five (5) point Likert scale ranging from 1= Strongly Disagree (SDA), 2 = Disagree (DA), 3 = not sure (NS), 4= Agree (A), 1= Strongly Agree (SA) and the findings are shown in table 9 below using Mean and Standard Deviation (SD).

Table 9: Descriptive Results for Company Processes

Company Processes	**Percentage**				**Mean**	**S.D**
	SDA	**DA**	**A**	**SA**		
Segregation of duties						
The separation of authorization function in transactions is adhered to	42.2	30.2	25	2.6	2.16	1.28
The separation of recording function, e.g. preparing source documents or code is adhered to	49.1	26.7	21.6	2.6	2.02	1.27
The direct and indirect separation of duties for custody of asset is adhered to	40.5	39.7	17.2	2.6	2.01	1.16

There is clear separation of reconciliation or audit functions in the company		12.1	57.8	13.8	3.75	0.85
Supervision						
The Board of directors exercise overall governance of the operational risk management in the company	45.7	33.6	18.1	2.6	1.98	1.19
The Audit committee exercises overall responsibility to take corrective actions on all identified operational risks	39.7	33.6	18.1	2.6	2.19	1.31
The management of Airtel exercises reasonable commitment and responsibility to implement all recommendations on operational risk	1.7	6.9	57.8	20.7	3.89	0.87
The law enforcement agents or stakeholders have been instrumental in managing operation risk	40.5	41.4	18.1	00	1.96	1.07
Reconciliations						
Monthly financial reconciliations reports are promptly submitted to the relevant authorities for action	1.7	8.6	47.4	30.2	3.96	0.96
The relevant stakeholders undertake to identify and investigate differences in financial transactions	1.7	10.3	46.6	28.4	3.90	0.99
Prompt corrective actions are taken in case of identified variances in financial transaction	3.4	6.9	40.5	34.5	3.96	1.04
All financial reconciliations are approved by management	12.1	20.7	47.4	19.8	3.75	0.91
Aggregated mean					**2.96**	**1.17**

Source: Primary data

The results in table 9 above revealed an aggregated mean of 2.96 which implied that the respondents agreed and as well as disagreed with the majority of the items of company processes in ORM. The Standard deviation ranged between 0.87 and 1.28, which was relatively narrow suggesting that most means did not deviate from the central mean by a big margin.

Item 9 which asked whether monthly financial reconciliations reports were promptly submitted to the relevant authorities for action and item 11 which asked whether the prompt corrective actions were taken in case of identified variances in financial transaction received the highest mean of 3.96 each suggesting that financial reconciliations were adequately undertaken through generations of financial reports and taking of prompt corrective actions. However, item 8 which asked whether the law enforcement agents or stakeholders had been instrumental in managing operation risk received the lowest mean of 1.96 suggesting a low level of enforcement of identified

financial fraud which would help deter other staff who may wish to engage in illegal personal gains.

In the next subsection an item by item analysis is provided on each of the indicators of planning management functions of environmental analysis, schedule development and resource planning.

4.6.1. Segregation of Duties

Table 9 above shows that although a majority of 71.6% of the respondents agreed (mean = 3.75) that there was clear separation of reconciliation or audit functions in the company, majority of 72.4% disagreed (mean = 2.16) that the separation of authorization function in transactions was adhered to. A total of 75.8% disagreed (mean = 2.02) that the separation of recording function was adhered to, 80.2% disagreed (mean = 2.0) that the direct and indirect separation of duties for custody of asset was adhered to. These findings suggested that effective ORM was constrained by weaknesses in company processes related to inadequate segregations of duties leading to abuse of authorization, recording and custody of company assets principles compromising effective fraud management by the telecommunication company.

Asked to describe how segregation of duties affected ORM, the interviewees put it:

"Segregation of duties minimizes the risk of fraud and error as there is always a maker and checker for the various activities performed. It also encourages specialization thus efficient and effective means of operation"

4.6.2 Supervision

Table 9 above shows that majority of 79.3% of the respondents disagreed (mean = 1.98) that the Board of directors exercised overall governance of the operational risk management in the company while 73.3% disagreed (mean = 2.19) that the Audit committee exercised overall responsibility to take corrective actions on all identified operational risks. These findings suggested although the management of Airtel could have exercised reasonable commitment and responsibility to implement all recommendations on operational risk, the inadequate supervisions by the board of directors and audit committee to respond to audit recommendations and the use of law enforcement agents to act on detected high risk frustrated the company ORM processes which also constrains effective fraud management by the telecommunication company. It was necessary the board effectively observes its supervisory roles in the management of risk.

Asked to describe how segregation of duties affected ORM, the interviewees put it:

"Supervisions minimize errors and enforce optimal utilization of resources and helps enforce process conformance with guidelines"

4.6.3 Reconciliations

Table 9 above shows that the respondents agreed that the relevant stakeholders undertake to identify and investigate differences in financial transactions (mean = 3.90), while they also agreed that all financial reconciliations were approved by management (mean = 3.75). These findings suggested that Airtel strived to perform reconciliations by generations of monthly reconciliation reports and taking of corrective actions which go a long way in enhancing the effectiveness of the ORM through a financial reconciliation process which helps in enhancing the financial data integrity and financial loss prevention.

4.6.4 Correlation analysis between Company Processes and Financial Fraud Management

To test the relationship between company processes and financial fraud management Pearson's correlation analysis was conducted at the 2-tailed level and the findings are presented below.

Table 10: Correlation Matrix between Company Processes and Financial Fraud Management

Variable		**1**	**2**
Company Processes	Pearson Correlation	1	
	Sig. (2-tailed)		
Financial Fraud Management	Pearson Correlation	815.**	1
	Sig. (2-tailed)	.000	
**. Correlation is significant at the 0.01 level (2-tailed).			

$P \leq 0.05$

between company processes and financial fraud management suggesting that there was high positive significant relationship between company processes and financial fraud management. The implication was that effective financial fraud management in Airtel depends on company processes of effective segregation of duties, supervision and performance of financial reconciliations. Thus the segregation of duties, supervision and reconciliations processes if not well executed constraints the integrity of financial data, financial fraud reporting and financial loss prevention in the telecommunication sector. Through instituting of ORM processes of clear segregation of duties, it enables the apportioning of accountability for actions to specific persons and roles in financial fraud management while supervision aids in identifying deviations and taking of corrective actions in reconciliations in the telecommunication transactions thereby contributing to an efficient financial fraud management mechanism in the company.

The study therefore qualified the hypothesis that there is a significant relationship between company processes and financial fraud management in the Telecommunication Companies.

Asked to describe how company processes influence financial fraud management in Airtel the one interviewee put it:

"Company processes allow timely reconciliations lead to identification of errors and frauds which enables early and timely correction. Prevention of revenue loss, if error or fraud is detected early"

4.7 Multiple Regression Results

The purpose of the study was to examine the relationship between operational risk management and financial fraud management in telecommunication companies of Uganda. A multiple regression was undertaken helps understand how the typical value of the dependent variable changes when any one of the independent variables is varied, while the other independent variables are held fixed (Aldrich, 2005).

The multiple regression analysis was also used to describe the effect of training of personnel, company internal systems and company processes on financial fraud management and to identify which among the independent variables was a more significant predictor of the variance in the financial fraud management and to explore the forms of these relationships (Freedman, 2005). The findings of the multiple regression analysis are shown in table below.

Table 11: Multiple regression results between operational risk management and financial fraud management.

Adjusted R^2 = 0.780		Un-standardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta β		
1	(Constant)	.820	.183		4.483	.000
	Training of Personnel	.188	.076	.173	2.479	.011
	Internal Systems	.604	.083	.694	7.309	.000
	Processes	.362	.070	.365	5.180	.000
Dependent Variable: Fraud Management predictors: personnel, internal systems & processes						

Source: Primary data

Table 11 above shows an adjusted R^2 value of 0.780 between operational risk management aspects of training of personnel, internal systems and processes suggesting that operational risk management predicted 78.0% of the variance in financial fraud management while other variable predicted the remaining 21.7% of the variance in the financial fraud management.

The company internal systems operational risk management aspect had the highest influence on the status of financial fraud management (β = 0.694, t = 7.309, and sig = 0.000). This was followed by company processes of segregation of duties, supervision and financial reconciliations (β = 0.365, t =5.810, and sig = 0.000). Personnel training although the least ORM factor was never the less a significant predictor of the variance in financial risk management (β = 0.173, t =2.479, and sig = 0.015). The implication was that any efforts to effectively manage fraud in telecommunication firms needs to give priority to internal systems related to network connectivity, ability to access logs and perform audit trails and effective records management and maintenance. The observance of effective company processes related to segregation of duties, supervision and reconciliations should equally be emphasized without compromise of training of employees.

CHAPTER FIVE

SUMMARY, DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary, discussion, conclusions and recommendations of the study on ORM and financial fraud management. The first section presents a summary of the study findings in relation to the specific objectives. This is followed by a discussion, conclusion, and recommendations of the study in relation to the objectives of the study. Limitations of the study, contributions of the study and recommendations for further studies are equally presented.

5.2 Summary of the study findings

This sub section presents a summary of the study findings on the relationship between personnel training, internal systems, company processes and fraud management.

5.2.1. Training of Personnel and Financial Fraud

The study found out that ORM training needs assessment mostly emphasized departmental risk management needs. However, most employees did not possess adequate IT skills necessary for effective management of operational risk at their level which reduces their effectiveness in ensuring financial data integrity, financial reporting and financial loss prevention.

The study found a high positive significant relationship between personnel training aspects of training needs assessment (TNA) and employee competencies and fraud management in Airtel qualifying the hypothesis that there is a significant relationship between training of personnel and financial fraud management in the Telecommunication Companies.

5.2.2. Internal systems and Financial Fraud Management

The study found out that authentication of users to access transaction records was the most emphasized to help track users actions and accountability for their actions. However, the study found out that user were most constrained by inadequate records management system necessary to effectively audit transactions at their level which reduces their effectiveness in identifying and mitigating financial fraud.

The study found a high positive significant relationship between company internal systems of network connectivity, access logs, records management and fraud management in Airtel qualifying the hypothesis that there is a significant relationship between company internal systems and financial fraud management in the Telecommunication Companies.

5.2.3. Company processes and Financial Fraud Management

The study found out that financial reconciliations were the most adequately considered and undertaken processes through generations of financial reports and taking of prompt corrective actions. However, the study found a low level of enforcement of identified financial fraud which would help deter other staff who may wish to engage in illegal personal gains.

The study found a high positive significant relationship between company processes of segregation of duties, supervision and reconciliation and fraud management in Airtel qualifying the hypothesis that there is a significant relationship between company processes and financial fraud management in the Telecommunication Companies.

5.3 Discussion of the study findings

This sub section presents a discussion of the study findings on the relationship between ORM practices of personnel training, company internal systems, company processes and fraud management in relation to what other scholars have observed.

5.3.1. Training of Personnel and Financial Fraud Management

The study found out that ORM training needs assessment mostly emphasized departmental risk management needs. However, most employees did not possess adequate IT skills necessary for effective management of operational risk at their level which reduces their effectiveness in ensuring financial data integrity, financial reporting and financial loss prevention. The identified skills necessary to effectively perform financial fraud management relate to Apostolou (2000) proposition for possession of legal elements and which law to apply for persons conduction financial fraud.

Training of personnel training aspects of TNA and employee competencies had a significant relationship with fraud management qualifying the hypothesis that there is a significant relationship between training of personnel and financial fraud management in the Telecommunication Companies. This study position is supported by Comision (2003) observation that an organization's control environment can be seriously eroded if a significant number of positions are filled with persons lacking required job skills and recommends that adequate training should be available to help employees until proper skills are acquired. In support, The COSO (2004) framework posits that Risk Management Training is important for improved internal control quality. In support, Farrugia (2002) asserts that staff training is a key element in risk management and one that needs constant reappraisal with regard to the type of risk and design of

controls as organizations operate in a dynamic environment. Kramer (2003) too argued that employees who are actively trained in risk management are likely to more accurately identify threats to the organization as a result of weak or non-existent internal controls.

It rests on the management of the telecommunication firms to ensure adequate training needs identification and development of appropriate training programs to equip staff with the necessary competencies for effective fraud management at the different levels in the company.

5.3.2. Company internal systems and Financial Fraud Management

The study found out that authentication of users to access transaction records was the most emphasized to help track users actions and accountability for their actions. However, the study found out that user were most constrained by inadequate records management system necessary to effectively audit transactions at their level which reduces their effectiveness in identifying and mitigating financial fraud. Stock (1999) observation in relation to the company internal sytems was of the view that information systems produce reports, containing operational, financial and compliance-related information that makes it possible to run and control the business.

The study found a high positive significant relationship between company internal systems of network connectivity, access logs, records management and fraud management in Airtel qualifying the hypothesis that there is a significant relationship between company internal systems and financial fraud management in the Telecommunication Companies. These study findings echo McNamee (1999) observation that risk assessment is a tool to help to detect and deal with fraud in operations of organizations. Some scholars had highlighted the role of the internal audits and noted that the effectiveness of this function may be attributable to the reasonable use of and compliance with internal auditing standards (Leung &Cooper, 2009; Abdolmohammadi, 2009). Furthermore,

others have noted that an effective internal audit function can provide advance notice of fraud risk, thereby helping to detect and prevent fraudulent financial reporting (Gramling & Myers, 2003; Rae & Subramaniam, 2008; Peterson & Gibson, 2003). It was necessary that telecommunication company guarantees network connectivity, secure access logs and provide for multiple, documentation to enable exertion of operational risk management activities for effective financial fraud through contingence interventions.

5.3.3. Company processes and Financial Fraud Management

The study found out that financial reconciliations were the most adequately considered and undertaken processes through generations of financial reports and taking of prompt corrective actions. However, the study found a low level of enforcement of identified financial fraud which would help deter other staff who may wish to engage in illegal personal gains. Previous studies are in agreement with this study findings and posit that authorization and approval, arithmetical and accounting procedures, segregation of duties, chart of accounts, system manuals, physical controls and independence checks (Arens & Loebbecke 1997, Ishungwa, 2001; Steinberg & Tanki 2005). Campion (2000) noted that when assessing the need for processes and procedures, the Board should consider whether it has other means of obtaining sufficient and objective assurance regarding the effectiveness of the system of the processes.

The study found a high positive significant relationship between company processes of segregation of duties, supervision and reconciliation and fraud management in Airtel qualifying the hypothesis that there is a significant relationship between company processes and financial fraud management in the Telecommunication Companies. In support, Comision, (2003) contends that management ensures where practicable, policy formulation, supervisory and other internal process review or advisory functions, including where applicable compliance and internal audit, are effectively

segregated from line operational duties. Such segregation serves to ensure the effectiveness of supervisory and other controls on financial fraud management established by management. Ashbaugh-Skaife, et al., (2006) argue that firms with operational risk management deficiencies have higher idiosyncratic risk. The higher the idiosyncratic risk, the more likely a firm will experience a large drop in reputation, which typically triggers shareholder class-action lawsuits. Within organizations, the hierarchical position may either limit or facilitate certain types of fraud (Holtfreter, 2005). Executives and owners may also have more authority to override existing controls than lower level employees, thus allowing the fraud to grow and go undetected for a longer period of time than other frauds (ACFE, 2008; KPMG, 2009). In retrospect, Peltier-Rivest and Lanoue (2012) study concluded that designing and implementing controls which mitigate the risk of collusion to reduce the increased losses that normally result from such frauds is essential for organizations. Simple controls, such as segregation of duties and anonymous reporting hotlines, may very well prevent and detect large frauds before financial damages irrevocably harm the organization.

This above discussion inferred that effective fraud management in telecommunication companies will depend on how segregation of duties, supervisions and reconciliations are undertaken by the telecommunication firm.

5.4 Conclusions of the study findings

This sub section presents conclusions of the study findings in training of personnel, internal systems, company processes aspects of ORM and financial fraud management in telecommunication companies based on the study findings and discussions above.

5.4.1. Training of Personnel and Financial Fraud Management

The study concluded that conducting of operation risk focusing on identification of employee training needs and development of employee knowledge and skills significantly influences financial data integrity, financial fraud reporting and reduces financial loss thereby contributing to financial fraud management in telecommunication companies.

5.4.2. Company internal systems and Financial Fraud Management

The study concluded that conducting of operation risk focusing on company internal systems of network connectivity, access logs, records management and maintenance significantly influences financial data integrity, financial fraud reporting and reduces financial loss thereby contributing to financial fraud management in telecommunication companies.

5.4.3. Company processes and Financial Fraud Management

The study concluded that conducting of operation risk focusing on company processes of segregation of duties, supervision and reconciliations significantly influences financial data integrity, financial fraud reporting and reduces financial loss thereby contributing to financial fraud management in telecommunication companies.

5.5 Recommendations of the study findings

This sub section presents recommendations of the study findings on training of personnel, company internal systems, processes and financial fraud management in telecommunication companies in Uganda based on the study findings and conclusions.

5.5.1 Training of Personnel and Financial Fraud Management

The study recommends that to achieve the desired level of financial data integrity, financial fraud reporting and mitigation of financial loss, the management of telecommunication companies should continuously identify operational risk management annual training needs at the individual level without compromise of the departmental and unit levels. This should be complemented with development of training programs to impart employees at the different levels with knowledge of telecommunication operations risk procedures, operational risk management regulations, advanced account, operations risk communication and strong IT skills.

5.5.2 Company internal systems and Financial Fraud Management

The study recommends that to achieve the desired level of financial data integrity, financial fraud reporting and mitigation of financial loss, the management of telecommunication companies should continuously ensure network connectivity and data backup and storage alternative. This should be complemented by strengthening of access logs and trails through segregation of roles of all actions by users, and protection of audit trails from the manipulation by other users. Enhancement of the records management system by collecting reasonable information, secure storage and retrieval through use of paper and electronic transaction records management system is equally recommended.

5.5.3 Company processes and Financial Fraud Management

The study recommends that to achieve the desired level of financial data integrity, financial fraud reporting and mitigation of financial loss, the management of telecommunication companies should enhance its internal controls by segregations of duties by adhering to separation authorization, recording and maintaining of an assets policy. This should be complemented with effective supervision of management actions by the board and exercises of overall responsibility to take corrective actions on all identified operational risks by the audit committee.

5.6 Limitations of the study

The study relied on primary data collected using a standardized questionnaire and interview guide without use of secondary data to effectively triangulate and enhance the data quality. Similarly, the use of one case study of Airtel Uganda limits the generalization of the study findings to other telecommunication companies.

5.7 Contributions of the study

The study makes managerial and operational risk management recommendations for enhanced financial fraud management demanding the for identification of staff training needs assessment, development of staff competencies in ORM, strengthening of access logs and trails through segregation of roles of all actions by users to enhance the company internal systems. Similarly, the study has also helped cover literature gaps by providing empirical evidence on the relationship between operational risk management dimensions of training of personnel, internal systems, company processes and financial fraud management.

5.8 Recommendations for further studies

The study found out that operational risk management practices of training of personnel, internal systems, company processes and financial fraud management predicted 78.3% of the variance in financial fraud management while other variable predicted the remaining 21.7% of the variance in the financial fraud management. Other studies need to examine the role of regulatory policies on mitigation of financial fraud in the telecommunication sector.

References

Bryman, A. and Bell, E. (2007), Business Research Methods, 2nd edition, Oxford UniversityPress.

Campion, A. (2000). *Improving Internal Control A Practical Guide for Microfinance Institutions.* Eschborn: Sabine Eddigehausen,. Student litteratur, Lund, Sverige.

Chapman, C. and Ward, S. (2002), Managing project risk and uncertainty, John Wiley &Sons, Chichester, United Kingdom.

Chorafas, D. N. (2008), Risk Accounting and Risk Management for Accountants, CIMAPublication, Elsevier, United Kingdom.

CIMA Official Terminology (2005), Chartered Institute of Management Accountants, CIMA Publication.

Coates, B. E. (2003), Rogue corporations, corporate rogues & ethics compliance: The Sarbanes-Oxley Act, 2002. Public Administration and Management, 8(3), 164-185.

Collier, P. M., Berry, A. J. and Burkey, G. T. (2007), Risk and Management Accounting: Best

Practice Guidelines for Enterprise-wide Internal Control Procedures, CIMA Publishing,London.

Committee of Sponsoring Organization of the Treadeway Commission [COSO] (1992),Internal Control Integrated Framework, Committee of Sponsoring Organization of theTreadeway Commission, New York.

Committee of Sponsoring Organizations of the Treadway Commission [COSO] (2004),Enterprise Risk Management-Integrated Framework, AICPA, New York.

Cook, T. D. and Campbell, D. T. (1979), Quasi-Experimentation: Design and Analysis for Field Settings, Rand McNally, Chicago, Illinois.

Clikeman, P. M. (2003). *The Greatest Frauds of the Last Century.* Richmond: Richmond, VA 23173.

Commission, S. a. (2003). Management, supervision and internal control guidelines for persons licensed by or registered with the securities and futures commission. *Commission, Securities and Futures*, (p. 4). Hong Kong.

D'Archy, S. P. (2001). *Enterprise Risk Management.* Illinois: University of Illinois .

Dorfman, M. S. (2007). *Introduction to Risk Management and Insurance, 9th Edition.* Englewood Cliffs: Prentice Hall.

Fielder, F. E. (1964). *A Contingency Model of Leadership Effectiveness.* New York: Academic Press.

Gleim. (2008). *CIA Review Part1 & 2 13th Edition.* Florida: Gleim Publicatios Inc.

John, N. (2012). Accountant arrested in MTN Fraud Case. *Daily Monitor*, 1 and 4.

Leitch, M. (2004, October). *Interanal Ciontrol and leaking Profits*. Retrieved July 9th, 2012, from Internal Control Design: http://www.internalcontrolsdesign.co.uk/leakage/index.shtml

Leitch, M. (2008). *Intelligent Internal and Risk Management.* Hampshire GU11 3HR: Gower Publishing Limited.

Leitch, M. (2008). *Intelligent Internal Control and Risk Management.* Unified Solutions Limited.

Li, S., & Nadeem, M. (2010). *Risk Management and Internal Control.* Trollhattan: University West.

Marchetti, A. M. (2012). *Enterprise Risk Management Best Practices From Assesment to Ongoing Compliance.* New Jersey: John Wiley & Sons, Inc, Hoboken,.

Markowitz, H. M. (1952). Portfolio Selection. *Journal of Finance 7*, 77-91.

Mayers, D., & Smith, C. (1982). On the Corporate Demand for Insurance. *Journal of Business 55(2)*, 281-296.

Mbanga, J. (2012, May 24th). *How MTN lost mobile billions*. Retrieved July 11th, 2012, from the Observer: http://observer.ug/index.php?option=com_content&view=article&id=18921:how-mtn-lost-mobile-billlions&catid=78:topstories&Itemid=116

Mucunguzi, A. (2011, January 18). *Warid Telecom Faces PR Backlash Following Gender Insenstive Radio Commercial.* Retrieved May 31, 2012, from PC Tech Magazine: http://www.pctechmagazine.com/index.php?option=com_content&view=article&id=293:warid-telecom-faces-pr-backlash-following-gender-insensitive-radio-commercial&catid=1:latest-news&Itemid=162

Njoroge, R., Tay, K. L., & Ruhui, R. (2012). *Internal Audit Report Airtel Money Uganda.* PricewaterhouseCoopers Africa.

Panwar, A. (2009, November 01st). *Internal Controls: Aprimer For Small Businesses*. Retrieved July 10th, 2012, from DARE BECAUSE ENTREPRENEURS DO: http://www.dare.co.in/strategy/business-essentials/internal-controls-a-primer-for-small-businesses.htm

Peter L, B. (1996). *Against the Gods: The Remarkable story of Risk.* New York: John Wiley and Sons, Inc.

Poupart, O. (2010). *Risk management and internal.* Lafarge.

Schnider, A. (2009). Auditors Internal Control Opinions: do they influence judgements about investments. *Managerial Auditing Journal*, 24.

Simth, C., & Stulz, R. (1985). The Determinanats of Firms' Hedging Policies. *Journal of Financial and Quantitative Analysis 20*, 391-405.

Stock, M. (1999). *Internal Control: A Practical Guide.* London: Service Point (UK) Limited.

Telecom Italia . (2011, April 04th). Retrieved July 10th, 2012, from Telecom Italia Media: http://www.telecomitaliamedia.it/et/content/internal-control-system

Tushabe, D. F. (2012). Mobile Money Fraud on the Spotlight. *Summit Business Review*, 14-16.

Vroom, H. V., & Yetton, W. P. (1973). *Leadership and Decision Making.* Pittsburgh: University of Pittsburgh Press.

Woods, M. (2008). *A Contingency Theory Perspective on the Risk Management Control System Within Birmingham City Council.* Birmingham: Social Science Electronic Publishing, Inc.

Woodward, J. (1958). *Management and Technology.* London: Her Majesty's Stationary Office.

APPENDICES

Appendix I: Operational Risk and Financial Fraud Management Questionnaire

Introduction

This is a master's research work being undertaken for the Masters Management Studies (Financial Management) with the aim of deepening my understanding of operational risk management and financial fraud management that exist in Telecommunication Companies with focus on Airtel Uganda Limited. Any information given will be kept confidential. Thank you for your co-operation.

For purpose of clarity, operational risk management is defined a continuous, systematic process of identifying and controlling risks in all activities according to a set of pre-conceived parameters by applying appropriate management policies and procedures. This process includes detecting hazards, assessing risks, and implementing and monitoring risk controls to support effective, risk-based decision-making.

SECTION ONE: BACKGROUND INFORMATION

1. Education level: Diploma [ ] Degree [ ] Postgraduate [ ] Professional [ ]
2. Time worked with Airtel Uganda: Below 5 years [ ] 5-10 years [ ] 10-15 years [ ] 15 years and above [ ]
3. Job title: Heads of Department [ ] Senior Manager [ ] Manager [ ] Supervisor [ ] Regional Sales Team Leader [ ] Team contributor [ ]

SECTION TWO: OPERATIONAL RISK MANAGEMENT

Tick (√) on the scales of 1-5 how strongly you agree or disagree with the statements given.

Scale	1	2	3	4	5
	Strongly Disagree	Disagree	Not sure	Agree	Strongly Agree

OPERATIONAL RISK MANAGEMENT	**SD**	**D**	**NS**	**A**	**SA**
	1	2	3	4	5
Training of personnel					
Training Needs Assessment					
Airtel undertook to identify your operations risk management training needs necessary in the telecommunication sector of Uganda					
The identified operational risk training needs contribute to the existence of the company					

The identified operational risk training needs are relevant for the achievement of the objectives of your department					
The identified operational risk training needs are relevant to your roles and responsibilities in the company					
Knowledge and Skills					
You possess the necessary knowledge in capturing risk data at your level					
You possess the necessary knowledge in risk control assessment					
You possess the necessary knowledge in establishing indicators of key risks to the company operations at your level					
You possess knowledge of telecommunication operations risk procedures					
You possess knowledge of telecommunication operations risk applicable regulations					
You possess adequate accounting knowledge					
You have the ability to validate proper data for a specific risk analysis					
You are capable of communicating operational risk recommendations at you level					
You possess strong IT skills necessary to conduct operational risk analysis in the telecommunications sector					
INTERNAL SYSTEMS	**SD**	**D**	**NS**	**A**	**SA**
	1	**2**	**3**	**4**	**5**
Network connectivity					
The Airtel network connectivity is reliable in ensuring transactional data quality					
There are adequate alternatives to access transactional data in the event of network interruptions					
The network has clear data recovery mechanisms for the vital customer account information like account balance, account profile.					
There are adequate data backups to provide transactional data in the event of loss of a data source					
Access logs and Audit Trails					
There is an internal system which allows you to easily access the relevant chronological transactional records as documentary evidence for a specific operation					
Access to the transaction records is authenticated					
The internal system in Airtel provides for segregation of roles of all actions by users					
Audit trails of transactions performed by a user are protected from manipulation by other users					
Records management and Maintenance					
The internal system creates adequate records that you can use to audit transactions at your level					
The internal system can store adequate records that you can use to audit transactions at your level					
The internal system provides for adequate records security					
The internal system can adequately retrieve records necessary for risk analysis					

PROCESSES	SD	D	NS	A	SA
	1	2	3	4	5
Segregation of duties					
The separation of authorization function in transactions is adhered to					
The separation of recording function, e.g. preparing source documents or code is adhered to					
The direct and indirect separation of duties for custody of asset is adhered to					
There is clear separation of reconciliation or audit functions in the company					
Supervision					
The Board of directors exercise overall governance of the operational risk management in the company					
The Audit committee exercises overall responsibility to take corrective actions on all identified operational risks					
The management of Airtel exercises reasonable commitment and responsibility to implement all recommendations on operational risk					
The law enforcement agents or stakeholders have been instrumental in managing operation risk					
Reconciliations					
Monthly financial reconciliations reports are promptly submitted to the relevant authorities for action					
The relevant stakeholders undertake to identify and investigate differences in financial transactions					
Prompt corrective actions are taken in case of identified variances in financial transaction					
All financial reconciliations are approved by management					

SECTION THREE: FINANCIAL FRAUD MANAGEMENT

Tick (√) on the scales of 1-5 how strongly you agree or disagree with the statements given.

FINANCIAL FRAUD MANAGEMENT	SD	D	NS	A	SA
	1	2	3	4	5
Financial data integrity					
All generated financial transaction data in Airtel is always correct					
All generated financial transaction data in Airtel is always consistent					
All generated financial transaction data in Airtel is always complete					
All generated financial transaction data in Airtel is always accurate					
The financial report in Airtel is generally reliable and valid					
Financial fraud reporting					
Airtel has put in place appropriate financial fraud reporting policies					
Daily financial fraud reports are submitted to the relevant authorities for action by the responsible persons					
Weekly financial fraud reports are submitted to the relevant authorities for action by the responsible persons					

Monthly financial fraud reports are submitted to the relevant authorities for action by the responsible persons					
Quarterly financial fraud reports are submitted to the relevant authorities for action by the responsible persons					
Annual financial fraud reports are submitted to the relevant authorities for action by the responsible persons					
The relevant authorities take action on submitted financial fraud reports					
Financial loss prevention					
Airtel has adequately prevented financial loss arising from loss of stock					
Airtel has adequately prevented financial loss arising from revenue leakages					
Airtel has recorded a healthy financial growth					

Appendix II: Interview questions

1. Describe the ORM training needs assessment practices in Airtel
2. How competent are the staff in conducting ORM at their levels
3. What are the knowledge and skills challenges in ORM in the telecommunication sector of Uganda?
4. How does personnel training affect financial fraud management in Airtel Uganda
5. Describe how each of the following company internal systems affect ORM

- Network Connectivity
- Access logs &Audit trails
- Records management & maintenance

6. How does the above company internal systems affect financial fraud management in Airtel

7. Describe how each of the following company processes affect ORM

- Segregation of duties
- Supervision
- Reconciliations

8. How does the above company processes influence financial fraud management in Airtel

Appendix III: Table for determining sample size from a given population

N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	246
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	351
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	181	1200	291	6000	361
45	40	180	118	400	196	1300	297	7000	364
50	44	190	123	420	201	1400	302	8000	367
55	48	200	127	440	205	1500	306	9000	368
60	52	210	132	460	210	1600	310	10000	373
65	56	220	136	480	214	1700	313	15000	375
70	59	230	140	500	217	1800	317	20000	377
75	63	240	144	550	225	1900	320	30000	379
80	66	250	148	600	234	2000	322	40000	380
85	70	260	152	650	242	2200	327	50000	381
90	73	270	155	700	248	2400	331	75000	382
95	76	270	159	750	256	2600	335	100000	384

Note: "N" is population size

"S" is sample size.

Krejcie, Robert V., Morgan, Daryle W., "Determining Sample Size for Research Activities", Educational and Psychological Measurement, 1970