International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. VIII, Issue 5, May 2020

http://ijecm.co.uk/

ROLE OF IT RISK MANAGEMENT ON INSIDER FRAUD PREVENTION IN KENYA COMMERCIAL BANKS

Rose Mwai
MSc Candidate, Jomo Kenyatta University of Agriculture and Technology [JKUAT], Kenya
rrhouzek@gmail.com

Michael Kimwele
Lecturer Jomo Kenyatta University of Agriculture and Technology [JKUAT], Kenya

Karanja Ngugi
Lecturer Kenyatta University, Kenya

Abstract

Insider fraud is the use of one's occupational for personal enrichment through deliberate misuse or misapplication of the organisation's resources or assets. Association of Certified Fraud Examiners report that a typical organization loses at least 5% of its annual revenue through insider fraud. Reports from audit firms report that, in Kenya fraud contributes to 31.5% of the deterrents of global competitiveness. Banks in Kenya have automated most of their processes and are heavily relying on technology. Use of technology by banks presents avenues that can be exploited and lead to rise in insider fraud. The objective of the research was to investigate the effect of IT risks management on reduction of insider fraud in the Kenya banks. This was achieved by analysing IT risk assessment, IT risk awareness, IT risk audit and Information Security policy implementation as the key variables. The research's population was the 42 registered banks in Kenya targeting the information security managers, internal auditors and IT staff who are tasked with implementing IT risks management. Out of the 42 registered banks, responses were received from 26 banks representing 62% of the population. The respondents agreed that a reduction in insider fraud leads to improved bank financial performances reduces losses, spurs confidence and trust among customers and investors. The study discovered that

some banks had not adopted or had partially implemented these IT risk management measures The study recommends that all commercial banks in Kenya should adopt these IT risk management measures to reduce Insider fraud.

Keywords: IT Risks management, Insider fraud, IT risk audit, IT risk assessment, Information security policy, IT risk awareness

INTRODUCTION

Insider fraud is a widespread problem that affects every organization regardless of size, location or industry**.** Insider fraud is the use of one's occupational for personal enrichment through deliberate misuse or misapplication of the organisation's resources or assets. A typical organization loses at least 5% of its annual revenue through insider fraud reports Association of Certified Fraud Examiners. In Kenya, fraud contributes to 31.5% of the deterrents of global competitiveness reports audit firms. Commercial Banks in Kenya have automated most of their processes and are heavily relying on technology. As banks reliance on technology increases, the risks associated with technology use increases. Use of technology by banks also presents more avenues that IT savvy staff can exploit thus increasing technology risks that could lead to rise in insider fraud. The banking industry has employed various strategies to handle insider threat one of which is managing Information technology risks.

Information Technology (IT) use has replaced manual processes and related controls placed in banks' processes; as a result, IT-related frauds have increased. Data on fraud reported to the Banking Fraud and Investigation Department (BFID) indicates that fraud cases relating to computer, mobile, and internet banking are on the rise. Other fraud cases such as card fraud have also been attributed to computer-based online transactions that do not have effective preventive and detective controls (Central Bank of Kenya [CBK], 2014). Despite the significant adoption of CBK risk management guidelines by commercial banks in Kenya over half a decade (2005-2010), an alarming proportion of the commercial banks are concerned with fraud risk. The concern is mainly due to the rising losses from fraud by their employees and customers (PWC, 2011). ACFE highlights that there is a 48% chance of an employee committing fraud in the Sub-Sahara region yet few organizations have a department dedicated to fraud management.

IT Risks Management and Insider fraud

Insider fraud is the use of one's occupational for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets. Insider fraud follows a

certain pattern. Insider fraud can be a misappropriation of assets, corruption or financial statement fraud. People commit insider fraud mainly because of financial pressure, the opportunity to commit fraud and rationalization (ACFE, 2014). Globally, different measures are in place to handle frauds, laws have been formulated and most of the perpetrators jailed or fined for their actions. In spite of the measures in place, insider fraud is on the rise. Some of the causes of insider fraud are complacency of staff, lack of clear moral direction from senior management, known- independent audit department, poor management information, and greed (Frost, 2012).

Commercial banks in Kenya

A bank is a company, which carries or proposes to carry banking business in Kenya but does not include the Central Bank. Banking is the process of accepting money from the members of the public on deposit repayable on demand or after the expiry of a certain period. Banks represents a very significant and influential sector that contributes greatly to the global economy. Commercial banks in Kenya are licensed, supervised and regulated by CBK as mandated under the Banking Act (Cap 488). Some of the functions of commercial banks are to provide a safe place for clients to keep money, to facilitate the transfer of money from one account to another, to offer lending services, to offer customer investment services and assist in international trade (Kenyaplex, 2012). As indicated on the central bank of Kenya website, the banking industry in Kenya is comprised of 42 banks as of 31st March 2018.

Statement of the problem

According to the consolidated commercial banks' revenue for the year ended June 2015, it is estimated that commercial banks lose 5% of their revenue annually; this translates to a loss of Kenya 3.8 billion (CBK, 2015b). The actual loss due to insider fraud may not be known because the actual intent of the perpetrator is to keep the fraud secret. Regardless of whether the true loss is 5% or some other portion, the total financial impact of fraud amounts to hundreds of billions, if not trillions, of dollars each year (ACFE, 2014). It is estimated that 40-50% of organizations do not recover any losses suffered due to fraud (Keever, 2012). Unmitigated information technology risks lead to losses, this impact’s on the financial status of the banks and their reputation (Federal Financial Institutions Examination Council [FFIEC], 2015). Deloitte (2015) earmarked lack of customer or staff awareness, difficult to integrate data from different sources and inadequate fraud detection tools as the main factors that lead to insider fraud. As banks reliance on Technology increases, the risks associated with technology increases. If these risks are exploited they could lead to a rise in insider fraud.

PWC Global economic survey 2011 reported Kenya to be one of the countries in Eastern Africa with high incidences of fraud out of the 78 countries surveyed. 66% of organizations in Kenya are victims of economic crime; nearly double the global average of 34% (PWC, 2011). Increased rate of globalization combined with the expansion of technology has also increased the rate of fraud and introduced new fraud activities (Akelola, 2014). Recently, two commercial banks operations were detrimentally affected by fraud. Imperial Bank of Kenya collapsed after a multi-year fraud that cost the lender $380 million in bad loans and customer deposits (Daily Nation, Wednesday, Dec 14, 2016). Further, Chase bank was put under receivership due to insider fraud and the directors were charged with conspiracy to defraud the bank of billions of shillings, leading to its collapse in 2015. The directors defrauded the bank claiming that they had settled a loan to various companies worth Sh1.6 billion. Further, there were other fraud incidences perpetrated by the staff of the chase bank totalling hundreds of millions (Standard, Fri, July 21, 2017).

Some studies have been carried out concerning insider fraud and mitigation strategies. For example, Wanjohi (2014) conducted a study to establish fraud in the banking industry in Kenya. Luell (2010) also conducted a study to establish employee fraud detection under real-world conditions. Allison (2013) did a study to establish the insider fraud problem in the Jamaican government organization. Despite the massive inquiry into fraud and mitigation strategies, there is no study locally or internationally to establish the role of IT risk management on insider fraud prevention in Kenya commercial banks. This study sought to establish the role of IT risk assessment, IT risk awareness, information security policy implementation and IT risk audit on insider fraud in commercial banks in Kenya.

Research Objectives

The main objective was to analyse the role of IT risk management on insider fraud prevention in Kenyan commercial banks.

Specific Objectives

Specific Objectives of the research:

i). To analyse the effect of IT risk assessment on insider fraud in commercial banks in Kenya.

ii). To determine the effect of IT risk awareness on insider fraud in Commercial Banks in Kenya.

iii). To find out the effect of information security policy implementation on the state of insider fraud in commercial banks in Kenya

iv). To analyse the effect of IT risk audit on insider fraud in commercial banks in Kenya.

LITERATURE REVIEW

This research utilised these theories fraud triangle, competence motivation, expectancy theory, decision theory, acceptance and use of technology.

Fraud Triangle Theory

Fraud triangle theory suggests that in circumstances where fraud opportunity is low, fraud occurrence is low. Research indicates that one of the means of reducing fraud opportunity is implementing strong and effective management controls (ACFE, 2010; Said, J., Alam, M.M., Ramli, M., & Rafidi, M, 2017). The Fraud Triangle fraud states that fraud is dependent on three aspects; perceived incentives or pressures; perceived opportunities and rationalization of fraudulent behaviour. One of the recommended management controls is the use of assessment or audit to analyse staffs' behaviour. The three elements of the fraud triangle are influenced by the fraud perpetrators' psychology. Personal incentives and perceived pressure drive human behaviour. The need to rationalize wrongdoing as being somehow defensible is very much psychologically rooted in the notion of cognitive dissonance (Ramamoorti, 2008). Trusted persons become trust violators when they conceive themselves as having a financial problem which is not shareable and they think violating the position of financial trust could benefit them (Cressey, 2003)

In the context of this study, the theory offered a coherent and logical explanation of the cause of fraud. Further, it showed factors that contribute to success in fraud. The fraud triangle theory states that if the opportunity for perpetuating a fraud is reduced, fraud cases will reduce. The theory was applicable in this study to help ascertain whether the mitigation measures (IT risk management) employed by the banks helped to reduce fraud. This study sought to establish the effects of mitigation factors such as IT risk assessment, IT risk awareness, information security policy implementation and IT risk audit on insider fraud in commercial banks in Kenya.

The Routine Activity Approach

The Routine Activity Approach (RAA) is a sociological theoretical perspective that was developed by Lawrence Cohen and Marcus Felson in their effort to explain criminal trends in the United States between 1947 and 1974 as a result of changes in labor force participation and single-adult households (Cohen & Felson, 1979). The theory suggests that the organization of routine activities in everyday life constructs 'variable opportunity structures for successful predation. The conceptual framework of the theory consists of three minimal elements of direct-contact predatory violations' (Cohen & Felson, 1979), which were originally conceived to

address violent assaults or crimes where one person takes or damages the property of another (Willison & Backhouse, 2013). The three elements involve (1) a potential offender; (2) a suitable target and (3) the absence of capable guardians (see Figure below). These elements could be considered as three sufficient and necessary conditions for a crime to be committed. Their spatial and temporal convergence gives rise to the opportunity for crime. By implication, the theory implies that crime does not occur when there is a lack of even one of these elements (Willison & Backhouse, 2013).

Figure 1: Application of Routine Activity Theory in Crime

Source: (Cohen & Felson, 1979)

Quite often, organizations fall, victims of their employees, because they fail to take information security seriously, and so in this way, they ultimately create security loopholes that are ready to be exploited by insiders. This theory was applicable in this study since it relates to a behaviour approach to stopping a crime (fraud). Implementation of IT risk management system in commercial banks in Kenya would act as the first step towards prevention of insider fraud. This would further provide a huddle to those willing to commit fraud and therefore curb the motivation to commit a crime. Further, information security policy implementations plus the internal controls in the banks would act as guardian to prevent frauds in the commercial banks. Based on the theory, it is, therefore, hypothesize that IT risk management has no effect on insider fraud prevention in Kenya commercial banks.

Expectancy Theory

Expectancy theory indicates that an individual, in this case, a trainee will decide to behave or act in a certain way because they have certain expectations or outcomes associated with that

selected behaviour. They will be motivated to select a specific behaviour over other behaviours if their expectations will be fulfilled because of that selected behaviour. An individual may expect that there will be monetary or other intangible rewards for high performance like job satisfaction or career advancement. The theory alludes that staff will transfer the skills taught during training back to the job environment with a belief that this it will lead to better outcomes that can come in terms of job reward, satisfaction, and promotions (Jaidev, 2012). Expectancy is the faith that better efforts will result in better performance. Expectancy is influenced by factors such as possession of appropriate skills for performing the job, getting the required support for completing the job, availability of right resources and crucial information (MSG, 2008).

This study found its application since it alludes that individuals have different set goals and can be motivated if they believe that favourable performance will result in a desirable reward. Management must discover what resources, training or supervision that employees need. Training affects employees' behaviour, making them more competent to carry out their tasks. With the help of this theory, this research sought to find out how IT risk awareness is influencing the behaviour of staff members while adopting the IT risk management procedures in place.

Theory of acceptance and use of Technology

The theory of acceptance and use of technology explains the intention of a user to use an information system. It states that there are four determinants on how a user will use the information system; these are Performance expectancy, effort expectancy, social influence and facilitating conditions (Venkatesh, Thong, & Xu, 2012). Performance refers to the degree a user believes the system will assist them to achieve a particular goal. The influence is dependent on the age and gender of the user. Effort expectancy is the degree of ease of use of the system. Social influence is the degree a user is expected by others to use the system. Facilitating conditions refers to the degree the user believes that the organization and infrastructure exist to assist them to use the system (Sykes, Venkatesh, & Gosain, 2009). The figure below shows how the different factors influencing the acceptance and use of technology. Use of the acceptance and use of technology theory can assist banks while they are evaluating the effectiveness of IT risk awareness sessions as they review the implementation and use of IT risk policies and procedures. This theory can assist in answering the question; has the banks' staffs accepted the IT risk policies in place?

Adoption of IT risk management procedures to prevent fraud is based on the various expectations. The expectations include, whether the system will achieve the design goals, will be easy to use and that it will influence how people behave in the institution. Therefore,

expected that adoption of IT risk management procedures in a commercial bank will help prevent fraud and at the same time users in the bank will readily accept it.

Conceptual Framework

The conceptual framework acts as the blueprint of any research; it provides a rationale for predicting the relationship between the different research variables. The conceptual for this research shows the linkage between IT risk management and insider fraud with a specific focus on IT risk assessment, IT risks awareness, I.T risks audit and information security policy implementation.

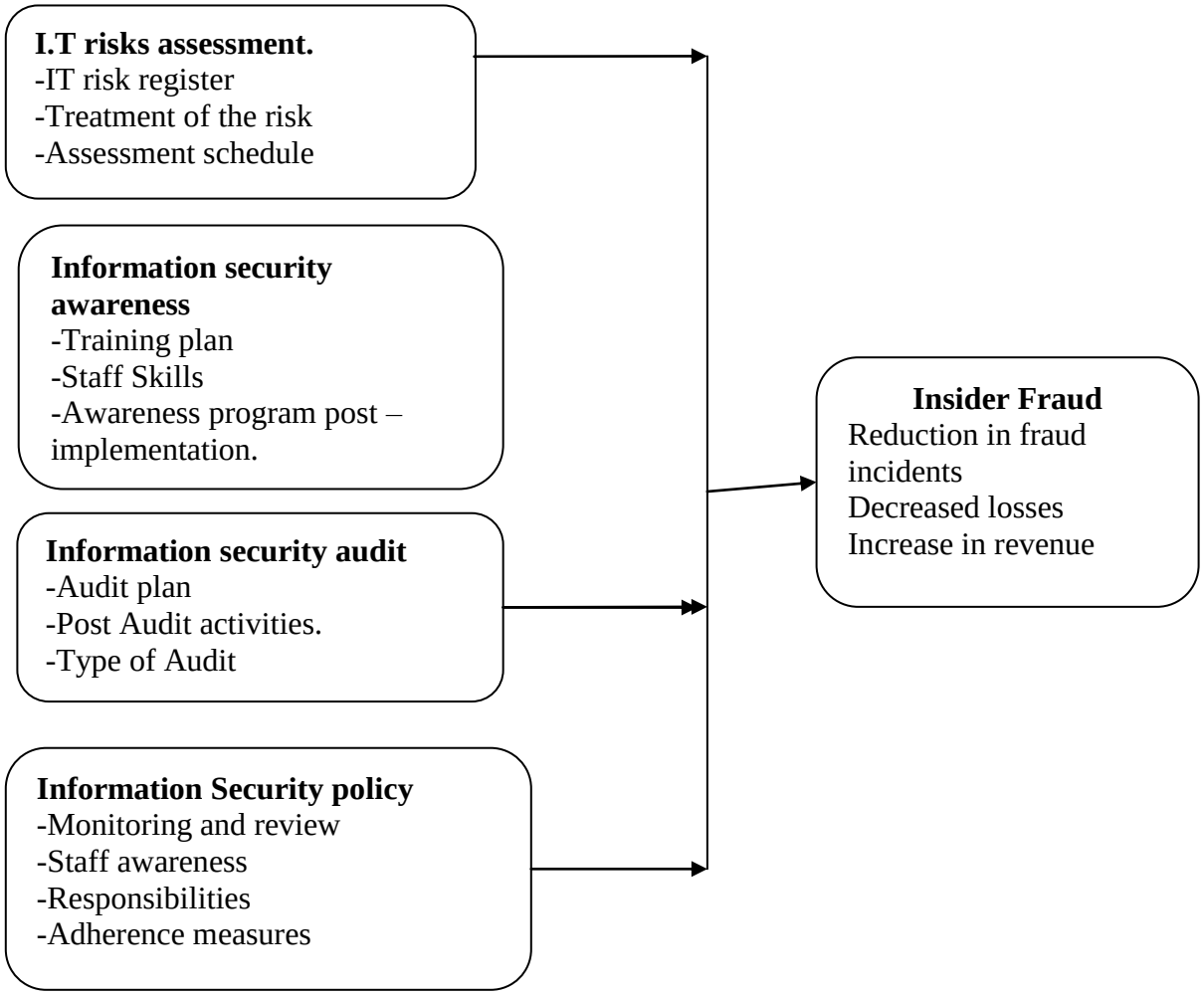

Figure 2. The Conceptual Framework.

EMPIRICAL REVIEW

This section covers a review of the work that other researchers have carried out in the area of IT risk management practices and insider fraud. It includes a literature review on the four research variables, that is IT risk awareness, IT risk system audit, IT risk assessment and IT risk policy implementation.

Insider fraud

Economic survey 2014 rated Africa as the region with the highest percentage of economic crime with 50% respondents indicating that they had experienced fraud. One in every four respondent in the survey reported to have experienced cybercrime and 11% of these reported a financial loss (PWC, 2014). Deloitte Forensic report indicated that frauds carried out by insiders have seen one bank lose money equivalent to Kenya Shillings 39 million and another 42 million (Nyamu, 2012). Kenya Bankers report on the trends of fraud in 2010 highlighted some of the threats faced by banks as a result of insider threat to be; cheque fraud, card (ATM, debit, and credit), forgery, wire transfers, counterfeiting, identity theft, embezzlement and loan fraud among others. The opportunities for insider attacks have increased. Most of the fraud cases involve bank staffs (Kenya Bankers Association, 2010).

Effect of I.T Risks Awareness on Insider fraud

The study on the effect of fraud in the banking industry in Kenya (Mulwa,2013) reported that most bank's had employed fraud mitigating strategies to some degrees however it highlighted proper training, awareness, motivation, and management of workplace issues like workload pressures could reduce fraud. The study reported that lack of staff security training was a challenge in nearly half (48%) of the banks in Kenya. Further, the report indicated that level of awareness of the customer had the greatest effect on the electronic fraud in the banking industry, followed by security controls, then quality management while the level of salaries and remuneration had the least effect to the electronic fraud in the banking industry (Mwabu, 2013).
Most fraudsters exhibit behavioural traits that can serve as warning signs of their actions such as living beyond their means. Managers, employees, and auditors should be educated on these common behavioural patterns and encouraged to consider them, to help identify patterns that might indicate fraudulent activity (Maurer, 2013). The purpose of fraud training is to inform employees of the many ways in which fraud can be perpetrated (Goettler & Banwart, 2007).

In spite of the availability of fraud prevention and detection measures such as anti-fraud controls, anti-fraud policy, formal management review procedures, anti-fraud training for staff members can be enacted with little direct financial outlay and provide a cost-effective

investment for protecting these organizations from fraud (ACFE, 2014). Staff should be trained on applying fraud mitigation procedures (Njenga & Osiemo, 2013). This research will seek to find out the adoption of the recommendations provided by (Njenga & Osiemo, 2013; Mulwa, 2013 and ACFE, 2014).

Effect of IT Risks Assessment on Insider fraud

The Statement on Auditing Standards (SAS) 99 of the American Institute of Certified Public Accountants (AICPA) emphasizes that auditors should exercise their professional scepticism to identify risks that may result in a material misstatement due to fraud. (Mulwa, 2012) the paper recommended that banks should regularly carry out a vulnerability assessment to prevent insider fraud. Vulnerability assessment should form part of the insider fraud response plan. Insider threat requires assessment, prioritization and the actions towards prevention should be in place rather than reaction. The information security program should contain a risk assessment process that maps the key risk indicators and link risk initiatives to corporate goals (Njiru, 2013).

ISO 27001 recommendations highlight that Information risk assessment is the first critical step in creating a comprehensive security program. A risk assessment is conducted by first identifying the information system assets of the organization, secondly identifying the risks associated with these assets and thirdly a probability of these vulnerabilities being exploited (Ng, Ahmad, & Maynard, 2013).

Effect of IT Risks Audit on Insider fraud

The study on determinants of insider fraud in commercial banks in Kenya by (Mahinda, 2012) reported that IT audit provides a vital role in the prevention, detection and investigation of fraud. A possible strategy for auditors in light of this problem is to assess the likelihood of fraud. The ability of an auditor to accurately assess the risk of fraud is crucial to the initial assessment of risk of material misstatement during the planning stage of the audit. Whether or not an auditor is auditing for fraud, all auditors are expected to assume responsibility for detecting fraud and assessing antifraud programs. Alinbashari, 2005 study of effects of fraud in the banking industry a case study of union bank Nig. Plc indicated that managerial supervision and reviews, including internal audit inspection are effective controls in fraud management. Increased situational awareness enables the risk assessment to incorporate internal changes and to react to expected changes in the threat landscape (E&Y, 2014).

Audited companies suffer less insider frauds reports ACFE reports to Nations on insider fraud. Internal or external auditors can carry out audit. The audit process is useful because in

itself fraud can be detected through routine procedure such analysis of data trends and assets. Secondly, the presence of auditors discourages employees from committing fraud in the first place (ACFE, 2012). The US Public Company Accounting Oversight Board (PCAOB) also requires auditors to evaluate fraud-related activities as a component of an internal audit function (ISACA, 2008).

In strategies adopted by commercial banks in Kenya to combat fraud: a survey of selected commercial banks in Kenya Mwithi & Kamau (2015) it was noted that inadequate auditing and placing too much trust on key employees could cause high risk of frauds and money laundering. The study further indicated that an internal audit is one of the fraud control mechanism that financial organizations should adopt.

The ACFE 2014 report on insider fraud and abuse indicated that 16% of the organizations in Sub Sahara region have implemented internal audit as a fraud deterrent method. The ACFE 2014 report further indicated that internal audits enabled 16.5% of the organisations in the survey with over 100 staff members to capture fraud. While independent audits serve a vital role in organizational governance, they should not be relied upon as organizations' primary anti-fraud mechanism (ACFE, 2014).

Effect of Information Security Policy Implementation on Insider fraud

In the study, a framework to Guide Security Initiatives for banking systems (Njiru, 2013) highlighted that one of the controls that banks in Kenya should employ in mitigating system threats was the use of security policies. The respondents in the study agreed that this was very critical to help banks protect their reputation. Further, the paper recommended that banks should include an Information Security policy in their Information security framework, Examples of Information Security policy that have been implemented by banks is the whistleblowing policy. This policy has helped bank's combat frauds reports the study of determinants of fraud control measures in commercial banks, a survey of selected commercial banks in Nakuru town, Kenya (Sang, 2014). Anti-money laundering policy has enabled banks to mitigate insider fraud (Mwithi & Kamau, 2015)

Policies define and govern employees' behaviour. In its own; a policy document will not prevent insider threat; however, the consequences for lack of adherence should be clearly stated (Mulwa, 2012). For an Information Security policy to be effective, it should be incorporated into the overall corporate risk management policy (Corpuz & Barnes, 2010). The main goal of a corporate Information Security policy is to protect data by defining procedures, guidelines, practices for configuring and managing IT risk in the corporate environment. The

policy must define the organization's philosophy and requirements for securing information assets (Whitman M E, Mattord HJ 2009).

An information security policy can reap several benefits to an organization, which includes; reduced vulnerabilities, fortifying the IT infrastructure and provide business continuity. The trouble is that very few organizations take the time and trouble to create decent policies; instead, they are happy to download examples from the web and cut and paste as they see fit as and organizations are left to unforeseen issues. (Scott, 2013). Under the Central bank of Kenya risk management guidelines 2013, each bank is required to have an Information security policy in place for mitigating IT risks. For any information security management program to succeed, the policies and procedures set must be frequently revised.

Critique of the existing literature

Mulwa (2013) in a survey of insider information security threats management in commercial Banks in Kenya (Mulwa, Dominic K, 2012) carried out an analysis of insider threat faced by commercial banks in Kenya and how banks can implement different policies and controls to mitigate these threats. He suggested the following measures to be implemented: training of staff, motivating, creating awareness and Time management. Mulwa (2013) addressed the issues faced when banks are implementing information security however he didn't address how effective these measures are in reducing the effect of insider fraud.

Jimmy Mutuku Mwithi, 2015, study of strategies adopted by commercial banks in Kenya to combat fraud: a survey of selected commercial banks in Kenya, recommends that staff training should be done. The study provided a list of measures to be implemented by banks while mitigating general fraud, however the study did not carry out an analysis Stella Wanjiru Njiru, 2013, studied a Framework to Guide Information Security Initiatives for Banking Information Systems: Kenyan Banking Sector Case Study, she concentrates on analysing information security frameworks that banks in Kenya have adopted. She recommended a further study in incorporating information security management as part of the business strategy. Some of the earlier studies have focused on particular aspects of computer fraud like insider fraud, electronic fraud but no study have been done on information security management as a discipline and how the banks can benefit from adopting an InfoSec program using a top-down methodology. Investigating information systems security for banks in Kenya (Gakure, Silas T 2008) looked at challenges commercial banks in Kenya face while implementing and adopting information security frameworks.

Research has been carried out on control measures that should be implemented to control insider fraud however; there is no study on how IT risk management affects insider

fraud. (Gakure, 2008) looked at challenges commercial banks in Kenya face while implementing and adopting information security frameworks. Reports by ACFE, PWC and E& Y show indicate that banks' are replacing their manual banking processes with technology-driven solutions. This has introduced technology risks that did not exist a decade ago.

Research Gaps

Studies on insider fraud have focused on general strategies adopted, implementation of management control systems to handle fraud and not on the effect of technology risks management on fraud. Banks have adopted the use of technology to steam line their processes, services, and products. Technology, as we know, changes every day. Use of these technologies has introduced a new type of risk in the banking industry namely; the technology use risks. Technology risks present opportunities for insider fraud if not addressed. It is important to carry out a study on how technology risks management can affect insider frauds in commercial banks in Kenya. This research seeks to contribute to the available literature on how IT risks assessment, awareness, audit and policy implementation affects insider fraud in the banking industry in Kenya. Studies and CBK regulations have recommended that IT risks management should be implemented as a holistic corporate objective, the empirical review reveals that their little study has been carried out on how IT risks management is implemented in the banks.

METHODOLOGY

Research Design

Research design is the blueprint of any research that enables the researcher to come up with solutions to the problem in question (Nachmias & Nachmias, 2008). This research used exploratory and descriptive research methods. Descriptive research was used to describe the characteristics of the population of the study. It does not answer questions about how, when, or why the characteristics occurred. Rather it addresses the "what" question; what are the characteristics of the population or situation being studied (Patricia & Rangarjan, 2013). A descriptive study attempts to describe or define a subject, often by creating a profile of a group of problems, people, or events, through the collection of data and tabulation of the frequencies on research variables or their interaction as indicated by Cooper and Schindler (2008).

Descriptive research can be either quantitative or qualitative. To be able to achieve the objective, the effect of ITRM on insider fraud in banks, the study was mainly qualitative. Descriptive research was suitable for this study because it involves gathering data that describe events, organizing the data, depicting, tabulating it. Visual aids like graphs and charts were

used to represent the data. The unit of analysis of the research was IT risks management professionals in all the commercial banks in Kenya.

Population

According to Cooper and Schindler (2008), population refers to an entire group of objects/individuals having common observable characteristics. The 42 commercial banks in Kenya formed the population of the study. Individuals were sampled from this population forming the unit of observations; the level of analysis was the commercial banks. Questionnaires were distributed to 100 respondents in Kenya Commercial Banks. Of the 100 bank employees contacted for the study, thirty-one employees from twenty-six commercial banks responded with duly filled questionnaires of 62% response rate from the commercial banks.

Table 1 Response rate

Item	Commercial banks
Contacted	42
Returned	26
Response rate	**62%**

Sample Size

The sampling plan describes how the sampling unit, sampling frame, sampling procedures and the sample size for the study. The sampling frame describes the list of all population units from which the sample will be selected (Cooper & Schindler, 2008). Kombo & Tromp (2013) indicated that a sample is a finite part of a statistical population whose properties are studied to gain information about the whole. A sample should also be optimum one that fulfils the requirements of efficiency, reliability, and flexibility in terms of costs (Kothari, 2008). For the descriptive study, the sample should represent at least 10% of the targeted population (Mugenda, 2008), for this study, a target of 50% was sufficient and reliable. 26 banks responded representing 62% of the population.

Sampling Frame

According to Alan Bryman (2011), sampling frame describes the selection of the units from which the sample is selected. Sample frame was the 42 registered commercial banks in Kenya.

Sampling Technique

This study used purposive sampling to get a study sample. According to Saunders, Lewis, & Thornwill (2009), purposive sampling starts with a purpose in mind and the sample is selected to include people of interest and exclude those who do not suit the purpose. The purpose of the research was to find out if IT Risk management practices assists banks to reduce insider fraud. The people charged with implementing, reviewing Information security practices are internal auditors, Information security professionals and IT staff members.

Data Collection Instrument

For this research, questionnaires were used to collect the research data. The questionnaire was self-designed using the information collected during the literature review. The questionnaires were self-administered. The questionnaires were shared online through Google forms. The questionnaire contained open and close-ended questions. The questionnaire was divided into the following sections: general section IT risks assessment, IT risks awareness, IT risks audit, Information Security policy implementation. The general section sought to gather general information about the respondent i.e. age, the position of employment, skills, and terms of employment and the highest level of education. The other sections covered the different variables and sought to find out how these variables influence insider fraud in commercial banks' in Kenya.

Data Collection Procedure

The researcher informed the respondents that the instruments being administered were for research purpose only and the responses will be kept secret and confidential. The researcher sent the questionnaire through Google forms to the selected sample. To ensure a high response rate, follow up calls were being made to remind the respondents to complete the questionnaires. The researcher exercised care and control to ensure all responses to the questionnaires were recorded.

Pilot Testing

The researcher carried out pilot testing of the research instrument to check its reliability and validity. Bryman and Bell (2011) argued that a protest of the questions with suitable respondents could help to assess whether the questionnaire is going to cause any problems for respondents. The researcher selected a pilot group of 10 individuals from the population to test the reliability of the research instrument. According to Cooper and Schindler (2008), the pilot group can range from 10 to 100 subjects but it does not need to be statistically selected. The pilot study enabled

the researcher to familiarize themselves with the research and its administration procedure as well as identifying items that required modification. Pilot study helped the researcher to correct inconsistencies arising from the instruments to ensure that it met the researcher's objective.

Validity of the Research Instrument

To establish the content validity of the research instrument the researcher sought the opinions of experts in the field of study especially the researcher's supervisors and lecturers to facilitate the necessary revision and modification of the research instruments thereby enhancing validity.

Reliability of the research instrument

Cronbach's Alpha test was used to test the reliability of the research instrument. All the variables alpha coefficient results were higher than 0.7, according to Leech et.al (2006), this exceeds the minimum alpha coefficient of 0.7 which, indicates that the instrument was very reliable.

Table 2 Reliability statistics

Variable	Cronbach's Alpha	N of Items
I.T. risk assessment	.938	8
I.T. risk awareness	.812	7
I.T. risk audit	.794	4
I.T. security policy	.874	5

Data Analysis and Presentation

The study used both qualitative and quantitative data. Quantitative data collected through the questionnaires was reviewed for completeness, accuracy, and usability. The methodologies used to analyse the data collected were descriptive statistics and content analysis. Closed questions were analysed through the help of the statistical package for Social Science (SPSS) computer software. Regression was used to estimate the coefficients of the linear equation, involving one or more independent variables, which best predicted the value of the dependent variable. The researcher used multiple linear regression analysis to analyse the data. The regression model will be as follows:

$Y= \beta 0+ \beta 1X1+\beta 2X2+ \beta 3X3+ \beta 4X4+\alpha$

Y = Insider fraud

$\beta 0$ = Constant

β_1, β_2, β_3 and β_4 = Independent variables,

α = error term (normally distributed about a mean of 0 and for purposes of computation, the α is assumed to be 0).

X_1 = IT risks awareness

X_2 =IT risks assessment,

X_3 = IT risk audit

X_4 = Information Security policy implementation

FINDINGS

IT Risk assessment and insider fraud

The respondents were asked to what extent they thought IT risk assessment could reduce insider fraud in commercial banks in Kenya on a scale of 1 to 5 with 1 being not at all and 5 been a great extent. A majority of the respondent indicated largely at 54.8% while 29% of the respondents thought the effect of IT risk assessment on insider fraud to be largely. 12.9% of the respondents indicated that IT risk assessment would reduce insider fraud only to a little extent while 3.2% indicated that IT risk assessment would not lead to any reduction in insider fraud.

IT risk assessment helps in determining the risk treatment method had the second highest factor loading on insider fraud prevention at 0.910 followed by IT risk assessment involves identifying, evaluating, analyzing and managing risks had the third highest factor loading on insider fraud prevention at 0.881. Identification of threat, vulnerabilities, risk determination, likelihood, and impact analysis and control recommendation because of IT risk assessment had the fourth highest factor loading on prevention of insider fraud at 0.866. IT risk assessment helps in determining the risk treatment method had a factor loading of 0.835 on prevention of insider fraud while IT risk assessment helps in assessing, identifying and modifying the overall IT risk posture had the fifth highest factor loading on prevention of insider fraud at 0.825. IT risk assessment helps to identify and quantify the risks to the organization information assets in internal fraud control had the second least factor loading on prevention of insider fraud with a loading of 0.794. I.T risk assessment helps staff to have a collaborate view of the entire organization from an attacker's perspective; it had the least factor loading on prevention of insider fraud at 0.610.

The R-squared statistic of 0.643 means that IT risks assessment accounts for 64.3% of the variance in insider fraud. The overall regression model was statistically significant at 95% confidence level with and F-statistic of 20.396 ($p=0.00<0.05$). The regression co-efficient of 0.643 was significant with a p-value of $0.000<0.05$ indicating that a unit increase in IT risk

assessment leads to a 0.643 unit increase in organization agility as a result of reduction in insider fraud.

Table 3 Regression Analysis of IT risk assessment and insider fraud

Variable	B	Std. Error	t	sig
(Constant)	-8.197E-16	.140	.000	1.000
IT risk assessment	.643	.142	4.516	**.000**
F statistics(p value)	20.396 (**0.000**)			
R squared	**0.643**			

The overall model for effect of IT risk assessment on insider fraud was a represented below;

Insider fraud= -8.197E-16 + $0.643X_1$

Where;

X_1= IT risk assessment

IT risk awareness and insider fraud

The study sought to determine the impact of IT risk awareness on insider fraud in commercial banks in Kenya. The respondents were asked three questions. The first question asked the respondents their thoughts on whether IT risk awareness influences insider fraud in commercial banks in Kenya. 93.5% of the respondents thought that the IT risk awareness influences insider fraud in commercial banks while only 6.5% of the respondents indicated that IT risk awareness does not influence insider fraud in commercial banks. The respondents were asked on a scale of one to five to what extent they thought IT risk awareness influences insider fraud in commercial banks in Kenya with one being not at all and five being very great extent. 58.1% of the respondents indicated that IT risk awareness influences insider fraud to a great extent while 22.6% of the respondents indicated that IT risk awareness influences insider fraud to a very great extent while 12.9%% indicated IT risk awareness only influenced insider fraud to a moderate extent. 6.5% of the respondents indicated that IT risk awareness does not influence insider fraud at all as presented in table below.

To determine the effect of IT risk awareness on insider fraud, a linear regression model was fit on the data using the factor measuring IT risk awareness as the independent variable and the factor measuring insider fraud as the dependent variable. Results including the overall model fit, analysis of variance and the regression coefficients were presented below. The results show that IT risks awareness accounts for 38.6% of the variance in insider fraud. The regression model was also statistically significant at 95% confidence level backed by a

statistically significant F-statistic of 5.088 (p=0.032<0.05). The regression co-efficient of 0.386 was statistically significant at 95% confidence level with a p-value of 0.032<0.05. This indicates that a unit increase in IT risk awareness leads to a 0.386 unit increase in organization agility because of reduction in insider fraud.

Table 4 Regression analysis of IT risk assessment and insider fraud

Variable	B	Std. Error	t	sig
(Constant)	-8.197E-16	.140	.000	1.000
IT risk assessment	.643	.142	4.516	**.000**
F statistics(p value)	20.396 (**0.000**)			
R squared	**0.643**			

The overall model for effect of IT risk assessment on insider fraud was a represented below;

Insider fraud= -8.197E-16 + $0.643X_1$

Where;

X_1= IT risk assessment

IT Risk Audit and Insider Fraud

The study sought to determine the effect of the IT risk audit on insider fraud. To meet this objective, the respondents were asked to respond to two questions both on a five point likert scale. The first question prompted the respondent's opinion on what extent IT risk audit influences insider fraud in commercial banks in Kenya. The results indicated that 51.6% of the respondents believe that IT audit influences insider fraud to a great extent while 22.6% of the respondents believed that IT audit influences insider fraud to a moderate extent similar to 22.6% of the respondents who indicated that IT audit influences insider fraud to a very great extent. Only 3.2% of the respondents felt that IT audit influences insider fraud to a little extent. Overall, over 73% of the respondents indicated that IT audit influences insider fraud largely.

A linear regression model was fit using the factor measuring IT risk audit and the factor measuring insider fraud to determine whether IT risk audit has an effect on insider fraud. A review of the results indicated that overall, IT risk audit accounts for 67.7% of the variance in insider fraud. The regression model was also determined to be statistically significant at 95% confidence level with an F-statistic of 24.562 (p=0.000<0.05). The regression co-efficient of 0.677 was statistically significant at 95% confidence level with a p-value of 0.000<0.05. This indicates that a unit increase in IT risk audit leads to a 0.677 unit increase in organization agility because of reduction in insider fraud.

Table 5 Regression Analysis IT Risk Audit and Insider Fraud

Variable	B	Std. Error	t	sig
(Constant)	-6.878E-16	.134	.000	1.000
IT risk audit	.677	.137	4.956	**.000**
F statistics(p value)	24.562 (**0.000**)			
R squared	**0.677**			

The overall model for effect of IT risk audit on insider fraud was a represented below;

Insider fraud= -6.878E-16 + $0.677X_1$

Where;

X_1= IT risk audit

Information security policy implementation and Insider Fraud

The study sought to determine the effect that information security policy implementation has on insider fraud. To measure this effect, the respondents were presented with two questions on a five point likert scale. The first question asked respondents to what extent they think information security policy implementation influences insider fraud in commercial banks in Kenya. The results indicate that 41.9% of the total respondents believe implementation of Information Security policy implementation influences insider fraud in commercial banks largely while 25.8% of the respondents believe implementation of Information Security policy implementation influences insider fraud to by a very great extent similar to 25.8% who indicated the influence to be of moderate extent. Only 6.5% of the respondents believe that implementation of Information Security policy implementation influences insider fraud by little extent.

The factor measuring Information Security policy obtained from the factor analysis was regressed against the factor measuring insider fraud to determine whether Information Security policy has an effect on insider fraud. The results of the regression analysis presented in table below included the overall model fit, analysis of variance and the regression coefficients. The results indicated that overall, Information Security policy accounts for 59.6% of the variance in insider fraud. The regression model fit was observed to be statistically significant at 95% confidence level with an F-statistic of 19.959 ($p=0.000<0.05$). The regression co-efficient of 0.596 was statistically significant at 95% confidence level with a p-value of $0.000<0.05$. This indicates that a unit increase in Information Security policy leads to a 0.596 unit increase in organization agility because of reduction in insider fraud.

Table 6 Regression Analysis of Information Security policy implementation and insider fraud

Variable	B	Std. Error	t	sig
(Constant)	-5.720E-16	.147	.000	1.000
Information Security policy	.596	.149	3.995	**.000**
F statistics(p value)	19.959 (**0.000**)			
R squared	**0.596**			

The overall model for effect of Information Security policy implementation on insider fraud was represented below;

Insider fraud= -5.720E-16 + $0.596X_1$

Where, X_1= Information Security policy implementation

Role of IT risk management on insider fraud prevention

The objective of the study was to determine the effect of IT risk management on insider fraud in commercial banks in Kenya. Insider fraud was measured using a set of four questions on a five point likert scale question. The results were presented in table 7 below.

Table 7 Descriptive statistics on insider fraud

IT Risk management	Mean	Median	Mode
Reduction in insider fraud leads to improved bank financial performances	4.55	5.00	5
Reduction in insider fraud spurs confidence and trust among customers and investors	4.61	5.00	5
Reduction in insider fraud helps the commercial banks to reduce losses	4.58	5.00	5
Implementation of IT risk management has helped commercial banks reduce fraud significantly	4.23	4.00	4

The results above indicate that reduction in insider fraud leads to improved bank financial performances had a modal score of five similar to reduction in insider fraud spurs confidence and trust among customers and investors and reduction in insider fraud helps the commercial banks to reduce losses. This indicates that most of the respondents strongly agreed with these statements in relation to insider fraud. Implementation of IT risk management has helped commercial banks reduce fraud significantly had a modal score of four indicating that most of the respondents agreed with this statement in relation to insider fraud.

Multiple linear regression

The factors measuring the independent variables of IT risk assessment, IT risk awareness, IT audit and Information Security policy implementation were used in a multiple linear regression model with the factor measuring insider fraud as the dependent variable. The R-squared statistic of 0.745 indicated that 74.5% of the variance in insider fraud could be explained by IT risk assessment, IT risk awareness, IT audit and Information Security policy implementation.

The F-statistic of 8.086 with a p-value=0.000<0.05 indicates that the multiple linear regression model was significant at 95% confidence level. The analysis therefore indicates that IT risk assessment, IT risk awareness, IT audit and Information Security policy implementation are good predictors of insider fraud.

The results of the regression co-efficient indicate that IT risk assessment had a positive but statistically insignificant effect on insider fraud (r=0.366, p=0.082>0.05) while IT risk awareness had a negative but statistically insignificant effect on insider fraud (r=-0.247, p=0.214>0.05). IT audit had a positive and statistically significant relationship to insider fraud (r=-0.514, p=0.033<0.05) while Information Security policy implementation had a positive but statistically insignificant relationship to insider fraud (r=0.144, p=0.544>0.05).

The specific regression was presented as below:

Insider fraud= $-8.771E-16+ 0.336X_1 - 0.247X_2 + 0.514X_3 + 0.144X_4$

Where;

X_1= IT risk assessment

X_2= IT risk awareness

X_3= IT risk audit

X_4= Information Security policy

Table 8 Multiple Regression Model

Variable	B	Std. Error	t	sig
(Constant)	3.364E-01	.129	.000	1.000
IT risk assessment	.336	.186	1.810	.082
IT risk awareness	-.247	.194	-1.275	.214
IT risk audit	.514	.228	2.253	.033
Information Security policy	.144	.234	.615	.544
F statistics(p value)	8.086 (**0.000**)			
R squared	**0.745**			

SUMMARY OF THE FINDING

The study sought to find out if IT Risk management practices namely IT Risk assessment, IT Risk Audit, Information security policy implementation and IT risk awareness has an influence on insider fraud in banks. The respondents' feedback indicates that indicate that IT risk management influences insider fraud in commercial banks.

The respondents agreed that IT Risk assessment helps in assessing, identifying and modifying the overall IT risk posture to prevent insider fraud in the banks. Further, they indicated that IT Risk assessment helps to identify and quantify the risks to the organization's information assets and develop a risk register that informs the top management on the areas to focus on. With the risk register, the banks' are able to carry out risk assessment that helps in determining the risk treatment for insider fraud. In conclusion, the respondents agreed that I.T risks assessment helps staff to have collaborated view of the entire organization from an attacker's perspective.

The study sought to establish if the bank's has put in place an information security awareness program and the need for the program. The respondents agreed that Information security awareness programs help staff understand their responsibilities in preventing insider fraud incidences. In addition, the respondents agreed that for information security awareness to be effective banks should analyse the effect of awareness periodically. The research findings also indicated that the staff mandated with IT Risk management should have the skills they need to carry out their work. The research also showed that employees need information security awareness trainings since there is a greater risk of breaches occurrence because of ignorance, inconsistent risk tolerances, or carelessness. Changes in information technology and evolving IT norms on how, when, and where business operations occur necessitate the need for the awareness programs. In conclusion, the research findings showed that human failure" or "errors" is one of the most severe threats to information security hence the need for awareness programs.

In addition, the respondents agreed that to prevent insider fraud, IT security audits ensures that specified management action plans remain relevant and updated. Post audits reviews helps in identifying IT risks and impacts on reduction of Insider fraud incidents. In addition, the respondents' feedback supported that IT risk audit helps in timely detection of fraud and therefore directly influences the bottom line, reducing losses for an organization. The respondents agreed that audit helps in monitoring and measuring the efficiency and effectiveness of the risk management in place.

On information security policy implementation, the respondents said that they had signed different documents showing their responsibilities to information. Some of the documents

that they had signed were, non-disclosure, information security policy, email, access, computer acceptance, bring your own device, computer use acceptance, and Information systems security policy affirmation. Monitoring and reviewing staff activities against the information security policy help in reducing fraud. Information Security policy allows staff members to identify an acceptable risk level and this reduces losses faced due to insider fraud. Clearly communicating the information security policy to all staff members reduces insider fraud incidents. In addition, majority of the respondents agreed with the statement that information security policy has explicitly indicated the measures and controls in place to prevent or reduce insider fraud.

CONCLUSIONS

The research findings indicate that reduction in insider fraud leads to improved bank financial performances, spurs confidence and trust among customers and investors. Reduction in insider fraud helps the commercial banks to reduce losses. Implementation of IT risk management has helped commercial banks reduce fraud significantly. The study showed that IT risk audit and IT risk assessment had the greatest influence on insider fraud. Having a process of identifying the IT risks that affect the banks and tracking the mitigation measures helps the banks to know at a point in time their status. This in turn, allows the banks to reduce the opportunities for insider fraud.

Most of the banks have implemented regular IT Risk assessments schedule, some once per year and others every quarter. Post implementation review was highlighted as important in helping banks to understand their current state. On IT Risk awareness the study indicated that employees need IT Risk awareness training since there is a greater risk of breaches occurring because of ignorance, inconsistent risk tolerances, or carelessness. The effectiveness of these training sessions should be measured to ensure that they remain relevant.

Most of the respondents had signed the information security policy documents that acted as a guide on information security expectations. Staff activities should be monitored against the set information security policy guidelines, in order to reduce insider fraud. The respondents also indicated that most of their Information security policy did not indicate clearly the end users' expectations; this affected the effectiveness of the policy in reducing insider fraud.

AREA FOR FURTHER STUDIES

The reliability tests show that the independent variables; IT Risk awareness, IT risk audit and Information security policy implementation individually have an effect on Insider fraud. Correlation results showed that IT Risk Audit had the greatest influence on insider fraud.

Information security implementation and IT risk assessment also affected Insider fraud though not in a significant way. IT risk awareness had the least effect on insider fraud.

Further research should find out the other underlying factors that would make IT risk awareness have an insignificant effect on insider fraud. The variables considered in this research do not fully cover all the factors that affect insider fraud, therefore research can be carried out on why insider fraud is on the rise in commercial banks in Kenya. The research covered the commercial banks in Kenya; a study can be carried out on what Information Technology management has been implemented by micro finance institutions.

REFERENCES

ACFE. (2012). Report to the Nations on insider fraud and abuse. Association of Certified Fraud Examiners, Fraud Department. US: ACFE

ACFE. (2014). Report to The Nations on Insider fraud and Abuse. Association of Certified Fraud Examiners, Fraud Department. US: ACFE.

AFC. (2013) Audit & Risk Insight from Chartered Institute of Internal Auditors. [Accessed 28th February 2016] available from world wide web: http://auditandrisk.org.uk/news/afc-discusses-role-of-internal-audit-in-detecting-fraud

African Development Bank, A. (2015) African Development Bank; Information Technology Strategy 2012-2015.[Accessed 23rd January, 2016], Available from World Wide http://www.afdb.org/fileadmin/uploads/afdb/Documents/Policy-Documents/Information%20Technology%20Strategy%202013-2015%20-%20Revised.pdf

Akelola, D. S. (2014). Prosecuting Bank; Fraud in Kenya ; challenges faced by the Banking Sector. Journal of Finance and Management in Public Services, 14. 1

Alinbashari, U. I. (2008) Linköping Studies in Science and Technology, insider fraud –auditors' perceptions of red flags and internal control. [Accessed November 25th, 2015] Available from World Wide Web: http://liu.diva-portal.org/smash/get/diva2:235160/FULLTEXT01.pdf

Alan Bryman, Emma Bell (2011) Business Research Methods 3rd Edition Great Clarendon Street UK OUP Oxford press

Ayiekoh, Y. (2014) Banking Industry, Associated Risks and Mitigation Strategies. [Accessed January 16th 2016] Available from World Wide Web: http://www.scribd.com/doc/195895658/Banking-Industry-Associated-Risks-and-Mitigation-Strategies#scribd

Bailey et al. (1996) the language learner's autobiography: Examining the 'apprenticeship of observation'. In D. Freeman & J.C. Richards (Eds.), Teacher learning in language teaching. New York: Cambridge.

Boateng, A. A., Boateng, G. O., & Acquah, H. (2014). A Literature Review of Fraud Risk Management in Micro Finance Institutions in Ghana. Research Journal of Finance And Accounting,5, 42-51

CBK. (2013) Risk Management Guidelines. [Accessed 29th October 2015] Available from world wide web: https://www.centralbank.go.ke/images/docs/legislation/risk-management-guidelines-january-2013.pdf

CBK. (2015a). Performance and Development in the Kenyan Banking Sector for the Quarter ended 31st March 2015. Nairobi: Central Bank of Kenya.

CBK. (2015 b). CBK Annual Report for 2015. Nairobi: Central Bank Of Kenya.

Central Bank of Kenya (CBK). (2014). Bank Supervision Annual Report 2014. Nairobi: CBK, Kenya.

Corpuz, M., & Barnes, P. H. (2010) Integrating information security management with corporate risk management for strategic alignment. [Accessed 19th March 2016] available from World Wide Web: http://eprints.qut.edu.au/38217/

Cooper D. R., Schindler P.S. (2008) Business Research Methods. Mcgraw Hill Higher Education press 10th Edition

C.R. Kothari (2008) Research Methodology Methods and Techniques Newage publishers 2nd Edition

Cressey, D. R. (2003). Other People's Money: A Study in the Social Psychology of Embezzlement. Belmont CA: Textbook Publishers.

Deloitte (2015). India Banking Fraud Survey April 2015; Edition II. India: Deloitte.

E&Y (2014). EY's Global Information, Get ahead of cybercrime; EY Global Information Security Survey. UK: Ernst Young International.

Elliot, A. J., & Dweck, C. S. (2013). Competence and Motivation. In A. J. Elliot, & C. S. Dweck, Competence and Motivation Stanford: Guilford Press.

Federal Financial Institutions Examination Council [FFIEC]. (2015). FFIEC IT Examination Handbook Infobase. [Accessed 20th March 2016] available from World Wide Web http://ithandbook.ffiec.gov/it-booklets/information-security/information-security-strategy.aspx

Frost, K. (2012). Top 10 reasons why fraud occur. [Accessed 29th October, 2015] available from World Wide Web: http://metro.co.uk/2012/09/14/top-10-reasons-frauds-occur-3817555/

Gakure, S. T. (2008). Investigating information systems security for banks in Kenya. [Accessed 30th October 2015] available from World Wide Web: http://erepository.uonbi.ac.ke/handle/11295/23708

Goel, S., & Chengalur, S. I. (2010). Metrics for characterizing the form of security policies. The Journal of Strategic Information Systems 19, 281-295.

Goettler, J. L., & Banwart, H. (2007). Insider fraud and Abuse. [Accessed 30th October 2015] available from world Wide Web http://www.peoriamagazines.com/ibi/2007/oct/occupational-fraud-and-abuse

Howard, R., Thomas, R., & Winterfeld, S. (2010). Cyber Fraud Tactics, Techniques and Procedures. Boca Raton FL: CRC Press.

Jaidev, U. P. (2012). A Review of Theories that Support Transfer of Training. International Journal of Science and Research, 957

KEBS. (2014). Kenya Bureau of Standards . Retrieved January 24, 2016, from Kenya Bureau of Standards: http://www.kebs.org/index.php?opt=certification&view=isms

Ke-Cirt. (2016). Communication Authority of Kenya . [Accessed 23rd January 2016] World Wide Web http://www.ke-cirt.go.ke/index.php/about-us/

Keever, J. (2012, December 2). Key findings and highlights from the 2012 report on insider fraud and abuse. [Accessed 8th November 2015] World Wide Web http://www.insurancegateway.co.za/print//Kenya/PressRoom/ViewPress/URL=Key+findings+and+highlights+from+the+2012+report+on+occupational+fraud+and+abuse+2#.Vj9mYm5MRdg

Kombo, K. D. & Tromp, L. A. D. (2013). Proposal and Thesis Writing: An Introduction. Nairobi, KE: Pauline Publications Africa.

Kringen J.A., Felson M. (2014) Routine Activities Approach. In: Bruinsma G., Weisburd D. (eds) Encyclopedia of Criminology and Criminal Justice. Springer, New York, N

Lawrence E. Cohen and Marcus Felson Social Change and Crime Rate Trends: A Routine Activity Approach American Sociological Review 44 (4) 588-608

Mahinda, C. G. (2012) Determinants of insider fraud in commercial banks. [Accessed 28th November 2015] World Wide Web http://erepository.uonbi.ac.ke: http://erepository.uonbi.ac.ke/handle/11295/12977

Maurer, R. (2013, November 4). Fight Fraud with Employee Awareness. [Accessed 30th November 2015] World Wide Web http://www.shrm.org/hrdisciplines/safetysecurity/articles/pages/fight-fraud-employee-awareness.aspx

Mulwa, D. K. (2012, October). A survey of insider information security threats in commercial banks. [Accessed 12th January 2015] World Wide Web http://erepository.uonbi.ac.ke/

Mugenda, O., & Mugenda, A. (2008). The Method Section. In O. Mugenda, & A. Mugenda, Research Methods Nairobi AD Press.

Mwabu, D. K. (2013). Factors influencing electronic fraud in the banking industry in Kenya: a case of Kenya commercial bank central region (Doctoral dissertation, University of Nairobi). [Accessed 30th October 2015] World Wide Web http://erepository.uonbi.ac.ke/bitstream/handle/11295/60487/Mwabu_Factors%20Influencing%20Electronic%20Fraud%20In%20The%20Banking%20Industry%20In%20Kenya.pdf?sequence=3

Mwithi, J. M., & Kamau, D. J. (2015). Strategies Adopted by commercial banks to combat fraud, a survey of selected commercial banks. International Journal of Current Business and Social Sciences 2015(3), 1-18.

MSG. (2008) Management Study Guide, Expectancy Theory of Motivation – [Accessed November 8th 2015] from World Wide Web from Management Study Guide: http://www.managementstudyguide.com/expectancy-theory-motivation.htm

Nachmias, F., & Nachmias, D. (2008). Research Methods in Science 5th Edition. London: St Martin Press.

Nancy L Leech SPSS for Intermediate Statistics British Journal of Educational Technology 37, 973-990

Njenga, N., & Osiemo, P. (2013). Effect of fraud risk management on organization on organisations's performance, a case study of deposit taking microfinance institutions in Kenya, 2013. International Journal of Sciences and Entrepreunership 7, 1-23.

Ng, Z. X., Ahmad, A., & Maynard, S. B. (2013). Information Security Management; Factors that influence information security investments in SMEs. Edwin Cowan University Research Online 12, 60-73.

Nyamu, D. F. (2012). Kenyan Banks' Biggest Victims of Shs 4.1 Billion Fraud. [Accessed 30th October 2015] World Wide Web www.businessdaily.com: www.businessdaily.com

Njiru, S. W. (2013). A Framework to Guide Information Security Initiatives for Banking Information Systems: Kenyan Banking Sector Case Study. [Accessed 30th October 2015] World Wide Web https://su-plus.strathmore.edu/handle/11071/2336

Patricia, S., & Rangarjan, N. (2013). Integrating Conceptual Frameworks and Project Management. In S. Patricia, & N. Rangarjan, A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management (p. 161). 1018 S Lewis St, Stillwater: New Forums Press.

Potowski, K. (2007) Language and identity in a dual immersion school. Clevedon: Multilingual Matters.

PWC. (2014). Global Economic Crime Survey 2014 [Accessed 4th November 2015] World Wide Web http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/damage.html

Ramamoorti, S. (2008). The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component Into Fraud and Forensic Accounting Curricula. Issues in Accounting Education 23(4), 521-533.

Saunders M, Lewis P, Thornhill A (2009) Research Methods for Business Students Newyork Pearson Press

Said, J., Alam, M.M., Ramli, M., & Rafidi, M. (2017). Integrating ethical values into fraud triangle theory in assessing employee fraud: Evidence from the Malaysian banking industry. Journal of International Studies, 10(2), 170-184

Sang, M. J. (2014). determinants of fraud control measures in commercial banks, a survey of selected commercial banks in Nakuru town. International Journal of Science and Research 3.358, 2178 -2183.

Scott, A. (2013, April). Computer Weekly . [Accessed 20th March, 2016] World Wide Web http://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy

Sykes, T. A., Venkatesh, V., & Gosain, S. (2009). Model of Acceptance with Peer Support; A social Network Perspective to understand employees system use. MIS Quarterly 33, 371-393.

Willison & Backhouse (2013). Insider Fraud and Routine Activity Theory: A thought Experiment [Accessed 30th October 2015] World Wide Web https://www.researchgate.net/figure/Application-of-Routine-Activity-Theory-in-Crime-Source-Choo-2011_fig1_256457215

Whitman M E, Mattord HJ (2009) Principles of Information Security Cengage Learning EMEA , Canada.