International Journal of
Technology and Systems
(IJTS)

Role of ICT Risk Management on Insider Fraud Prevention in Commercial Banks in Nairobi County

Rose Wangui Mwai, Dr Samuel Wabala and Dr Ken Ogada

International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.8, Issue 2, No.3, pp 36 – 64, 2023

www.iprjb.org

Role of ICT Risk Management on Insider Fraud Prevention in Commercial Banks in Nairobi County

Rose Wangui Mwai
Post Graduate Student: Jomo Kenyatta University of Agriculture and Technology

Dr Samuel Wabala
Lecturer: Jomo Kenyatta University of Agriculture and Technology

Dr Ken Ogada
Lecturer, Jomo Kenyatta University of Agriculture and Technology

Article History

Received 10th September 2023

Received in Revised Form 22nd September 2023

Accepted 6th October 2023

How to cite in APA format:
Mwai, R., Wabala, S., & Ogada, K. (2023). Role of ICT Risk Management on Insider Fraud Prevention in Commercial Banks in Nairobi County. *International Journal of Technology and Systems*, *8*(2), 36–64. https://doi.org/10.47604/ijts.2135

Abstract

Purpose: The main objective of the research was to investigate the role of ICT risk management on reduction of insider frauds in the Kenyan banks in Nairobi County. The research explored ICT risks management practices incorporated in the banking industry to mitigate and control insider fraud.

Methodology: Explorative research design and inferential statistics were used. The unit of analysis was the ICT risk management professionals in all the commercial banks in Nairobi County. 42 commercial banks formed the population of the study. The unit of observation were the ICT security, audit and risk professionals mandated with implementing ICT risk management. The targeted number was at least one respondent from each bank from the three departments identified: internal audit, Information technology, and security managers. In total, the study targeted 42 respondents and a total 29 responses were received which formed 69% of the targeted population. Responses from the distributed questionnaires were analyzed using statical packages for social science (SPSS). The open-ended questions were listed, analysed and reported by descriptive narrative with such statistics as mean and standard deviation. The ANOVA test was used to test the results.

Findings: The findings revealed that there is a positive but insignificant correlation between ICT risk assessment, ICT awareness, Information security implementation and a significant positive correlation between information security audits and Insider fraud prevention. This study recommends that ICT risk assessment; ICT risk awareness; information security audits; and information security policy are important for preventing insider fraud in commercial banks, but there is need to implement them in conjunction with other stringent measure to increase efficiency

Unique Contribution to Theory, Practice and Policy: The findings give a theoretical basis for validating the effectiveness of ICT risk management practices in Banks in Nairobi County, this can be adopted by other counties in Kenya. For policy implementation, the study will be important to the central bank of Kenya and any other institution that regulates the banking sector in Kenya in reviewing the current ICT Risk management guidelines. The study shows the adoption of the selected ICT risk management practices by different banks and gives a measure of their effectiveness that ICT Security professionals can use. The study gives the banking sector ICT security professionals a perspective on how ICT risk management can help them improve their ability to curb insider fraud. The study adds to the pool of knowledge for to scholars and academicians.

Keywords: *Insider Fraud, ICT Risk Management, Banks*

INTRODUCTION

Insider fraud occurs when an employee makes a false representation, abuses a position of trust for personal gain or to cause losses to others, often it is referred to as internal or occupational fraud. (Fraud.net,2019). From the ICT perspective, Insider fraud is the potential of an insider to use their authorized access or understanding for personal gain (Ekran, 2021). Insider fraud can be caused by staff members not knowing the correct procedures and inadequate knowledge of the banks' products (Mwithi & Kamau, 2015).

Information Communication Technology (ICT) use has replaced manual processes and related controls placed in banks' processes; as a result, ICT-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 which do not have effective preventive and detective controls (Central Bank of Kenya [CBK], 2014). PWC 2020 report indicated that companies in Kenya have lost 5.5 billion Kenya shilling in economic fraud, insider fraud being one of the frauds (PWC,2020).

CBK as the regulator of all operating banks in Kenya has placed a requirement that every bank should have an information communication technology risk management function that will handle information technology risk issues (CBK, 2017). In the management of a business that makes use of ICT, it is important to identify risks to your ICT systems and data to reduce or manage those risks by developing a response plan.

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, 2020). ACFE highlights that there is a 48 percent chance of an employee committing fraud in the Sub-Sahara region yet few organizations have a department dedicated to fraud management.

In Kenya, various government organizations that handle different aspects of ICT risk. The Communication Authority of Kenya (CAK) through the Kenya Information and Communications Act, 1998, carries out analysis on computer security, incidences and manages Information security for the country (Ke-Cirt, 2016). Kenya Bureau of Standards (KEBS) Certification Body (CB) offers a Certification on ISO 27001:2013, (ISO/IEC 27000-series) "standards which provide good practice guidance on designing, implementing and auditing Information Security Management System (ISMS) to protect the confidentiality, integrity and availability of the information on which we all depend on" (KEBS, 2014).

Despite the presence of these regulations by CBK; computer frauds are on the rise. Some of the contributing factors are a rapid change in technology, computer-savvy users and lack of information security management programs in place. As Kenya embrace technology, technology risks have risen. Bank's statistics show that the frequency of internal fraud is increasing drastically and has by far inflicted most significant losses to the bank. This is because some dishonest employees and managers have found ways to override systems or collude with outsiders to defraud the banks (Waitumu, 2014). According to the Bank's fraud unit, management fraud occurs less frequently but accounts for the greatest financial losses. Position equals power; managers and executives who have high access rights have access to

more information and assets than regular employees, therefore, they can commit fraud relatively easy without being noticed (Njuguna, 2013).

The increase in types of risks, to which ICT systems are exposed to, implies that there is need for a systematic, repeatable and analytical approach to managing ICT risks (Njiru, 2013; Omolo, 2012). Kenya needs to invest in the space of technology management and especially technology risk management; information security is one of these. "Starting with policy to education and certification programs the country needs to put in concerted efforts to develop needed skills in this area to tackle/forestall looming problems. The country is lacking in ICT risk management risks, poor compliance regime and lack of leadership in technology "(Nyanchama, 2014).

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). The banking industry in Kenya is comprised of 42 banks as of 30th March 2022, 30 of these are locally owned and 12 are foreign-owned (CBK, 2021).

Statement of the Problem

In 2016, two commercial banks in Nairobi County operations were detrimentally affected by insider 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, December 14, 2016). Further, chase bank was also affected by insider fraud. The directors of Chase bank 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 totaling hundreds of millions (Standard, Fri, July 21st, 2017).

Increased rate of globalization combined with the expansion of technology has increased the rate of fraud and introduced new fraud activities (Akelola, 2014). Unmitigated information technology risks lead to losses, this impacts 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. ICTRM programs assist in managing technology risks. ICTRM program establishes an organizations risk appetite and mitigation procedures.

ACFE 2020 report on insider fraud in banking and financial services reported that in sub-Sahara 82 incidents were reported with a potential loss of $170,000. Banks continue to lose money because of insider fraud incidents, it is important for commercial banks to come up with

mitigation measures to reduce its occurrence. The researcher sought to find out if there are any ICT Risk management practices in place and their efficacy on preventing insider fraud.

Previous 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 insider 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 was important to carry out a study on how technology risks management could affect insider frauds in commercial banks in Nairobi County

Theoretical Review

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, 2020; 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 behavior (see Figure 1.2). One of the recommended management controls is the use of assessment or audit to analyze staffs' behavior. The three elements of the fraud triangle are influenced by the fraud perpetrators' psychology. Personal incentives and perceived pressure drive human behavior. 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 offers a coherent and logical explanation of the cause of insider fraud through the ICT risk assessments practices that seek to identify if risk exposure to Insider fraud. ICT risk assessments assist Banks to identify if these three elements of fraud theory exist, the measure of exposure and mitigation that have been implemented. The questions to measure the implementation of ICT risk assessment practices were formulated against these three principles of the fraud theory namely how are the opportunities for fraud measured, have they been exploited, what financial losses were faced by the banks.

The Organizational Culture Theory

The culture of an organization defines the shared behavior, beliefs, assumptions on how people in the organization should relate to each other and how work activities should be carried out. Culture includes the organization's vision, values, norms, systems, symbols, language, assumptions, beliefs, and habits (Selvalakshmi & Guru, 2017) Understanding the organisations culture enables the leaders to make right decisions and provide guidance. Organization's strategies are built around its culture. New staff may take time to understand an organization's culture but either way it should be clearly communicated through policies. These policies should be reviewed for effectiveness and completeness.

The three key concepts to look at when discussing the organizational culture of information security are staff conduct, change and context (Cano,2021). These three concepts are important

to understand in light of maintaining organization's culture in light of technological convergence. Through the use of this theory, implementation of Information security policy was defined. It helped answer the question, has implementation of an Information security policy assisted in changing the culture of the banks and as a result reduce insider fraud.

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 behavior. They will be motivated to select a specific behavior over other behaviors if their expectations will be fulfilled as a result of that selected behavior. 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 theory was used to assess the ICT risk awareness measure that have been adopted by different banks. The theory states that right motivation leads to favorable performance that leads to desired reward. Management must discover what resources, training or supervision that employees need. Training affects employees' behavior, making them more competent to carry out their tasks. With the help of this theory, the researcher was able to measure ICT risk awareness practices that include relevant training, measurement of the results on the staff behavior and reduction of loss due to insider fraud.

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.

In relation to this study, the theory was adopted to measure the implementation of Information security audit, it's effectiveness and ability to achieve the desired goals. The theory assisted in answering the question; has the banks' staff accepted the IT risk practices implemented by these commercial banks.

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 ICT risk management and insider fraud with a specific

focus on ICT risk assessment, ICT risks awareness, information security audit and information security policy implementation.

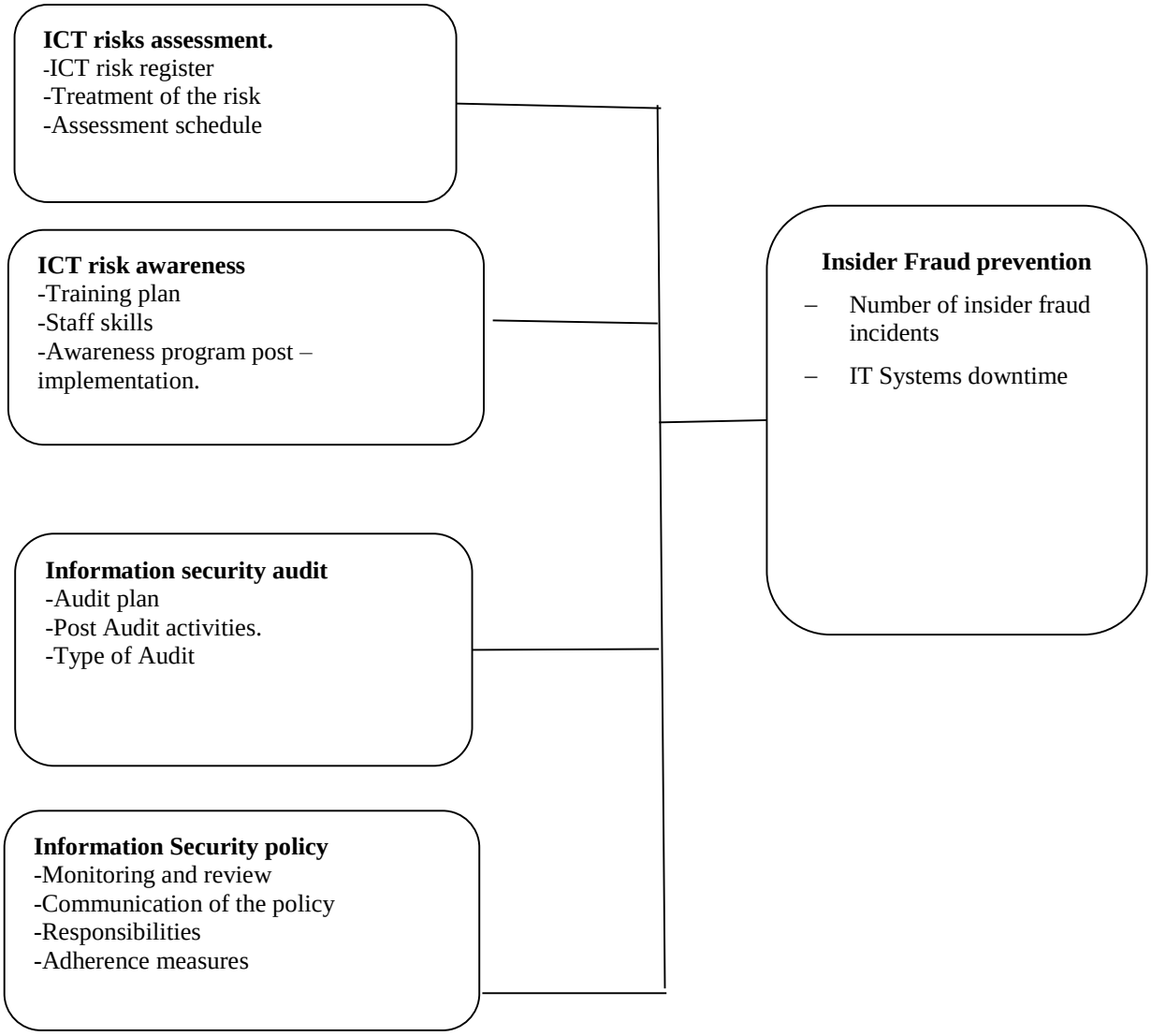

Figure 1: Conceptual Framework

Empirical Review

According to global risks report 2022, businesses are operating in a world in which 95% of cybersecurity issues can be traced to human error and insider threats. Kenya Department of Defense forensic (DFID) report on the trends of fraud in 2020 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).

The study on insider information security threats management in commercial banks in Kenya (Mulwa,2012) reported that most banks 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 behavioral 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 behavioral patterns and encouraged to consider them, to help identify patterns that might indicate fraudulent activity (Maurer, 2013).

Despite 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, 2020). Staff should be trained in applying fraud mitigation procedures (Njenga & Osiemo, 2013). This research sought to find out the adoption of the recommendations provided by (Njenga & Osiemo, 2013; Mulwa, 2012 and ACFE, 2020).

The Statement on Auditing Standards (SAS) 99 of the American Institute of Certified Public Accountants (AICPA) emphasizes that auditors should exercise their professional skepticism 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 which 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).

The study on determinants of insider fraud in commercial banks in Kenya by (Mahinda, 2012) reported that Information security 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, 2008 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. Audit can be carried out by internal or external auditors. 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, 2020). 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 mechanisms that financial organizations should adopt. The ACFE 2020 report on insider fraud and abuse indicated that 92% of the Banks and financial services have implemented internal audit as a fraud deterrent method. The ACFE 2020 report further indicated that internal audits enabled 60% of the organisations in the survey to reduce 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' behavior. 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 ICT 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 ICT 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 ICT risks. For any information security management program to succeed, the policies and procedures set must be frequently revised.

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 Nairobi County. This research seeks to contribute to the available literature on how ICT risks assessment, awareness, audit and policy implementation affects insider fraud in the banking industry in Kenya. Studies and CBK regulations have recommended that ICT risks management should be implemented as a holistic corporate objective, the empirical review revealed that little study has been carried out on the effectiveness of these ICT risks management practices in commercial banks in Nairobi County.

METHODOLOGY

The study used exploratory and descriptive research methods. The 42 commercial banks in Nairobi County 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 in Kenya. Questionnaires were distributed to three departments in the bank namely, internal audit, ICT, information security and risk management in each Commercial Banks in Nairobi County. The study was a census therefore it covered all the 42 registered commercial banks in Nairobi County. This study used purposive sampling to get a study sample. Questionnaire was used to collect the research data. The researcher sent the questionnaire through Google forms to the selected sample. The study used both qualitative and quantitative data. Quantitative data collected through the questionnaires was checked for completeness, accuracy and usability. The methodologies used to analyze the data collected was descriptive statistics and content analysis. Closed questions were analyzed through the help of the statistical package for Social Science (SPSS) computer software. The study used correlation to show the degree of association between the independent variables (ICT risks awareness, ICT risks assessment, Information security audit, and Information Security policy implementation) and the dependent variable (insider fraud prevention).

FINDINGS AND DISCUSSIONS

Descriptive Statistics

ICT Risk Assessment

The researcher sought to establish the extent to which they participants thought ICT risk assessment can reduce insider fraud in commercial banks. The findings are represented below.

Table 1: Extent to Which ICT Risk Assessment Can Reduce Insider Fraud

Extent	Frequency	Percentage (%)
Very great	15	51.7%
Great	13	44.8%
Little Extent	1	3.4%
Total	**29**	**100.0**

As shown in Table 1 above, the majority of the participants noted that ICT risk assessment can reduce insider fraud in commercial banks to a very great extent as represented by 15 (52.7%) of the participants. This was followed by 13 (44.8%) of the participants who noted that ICT risk assessment can reduce insider fraud in commercial banks to a great extent. It was only 1(3.4%) of the respondents who noted that ICT risk assessment can reduce insider fraud in commercial banks to a little extent. This implies that the majority believed in the effectiveness of ICT risk assessment in reducing insider fraud in commercial banks.

Additionally, the researcher sought to establish whether their organization has a schedule or program for assessing insider fraud and how regularly it is done. The findings are presented in Table 2.

Table 2: How Regular Assessing of Insider Frauds is Done

Extent	Frequency	Percentage (%)
Yearly	7	24.1%
Quarterly	15	51.7%
Half-yearly	3	10.3%
Others	4	13.8%
Total	**29**	**100.0**

The results show that various banks have different schedules for assessing insider frauds, where 7(24.1%) conduct the assessment on yearly bases; 15 (51.7%) on a Quartey basis; 3 (10.3%) on a half-yearly basis; and 4 (13.8%) indicated others. Those who indicated others comprised 1 (3.4%) who noted that he was not sure of the organization has a program or schedule; 1 (3.4%) who noted it is done regularly and there is no specific time applied; 1 (3.4%) who noted it is done based on fraud incident; 1 (3.4%) who indicated it is done on need basis; 1 (3.4%) that is done on monthly bases and in some cases on real-time bases; and 1 (3.4%) who note there is no such schedule or program to assess insider fraud.

Table 3: Descriptive Statistics for ICT Risk Assessment

Statements	1	2	3	4	5	Mean	Std. Dev
ICT risks assessment process helps in assessing, identifying, and modifying the overall ICT risk posture to prevent insider fraud	3.4	0	13.8	24.1	58.6	4.35	0.97
ICT risk assessment helps staff to have collaborate view of the entire organization from an insider fraudster perspective	3.4	0	17.2	31.0	48.3	4.21	0.98
ICT risk assessment involves identifying, evaluating, analyzing, and managing risks and thus helps prevent insider fraud	3.4	0	13.8	17.2	65.5	4.41	0.98
Identification of threat, vulnerabilities, risk determination, likelihood, impact analysis, control recommendation are benefits realized from ICT risks assessment that led to inside fraud prevention	6.9	0	17.2	20.7	55.2	4.17	1.17
Identifying the ICT risks that a bank is facing contributes to system availability and ensures that the bank is able to provide banking services to customers.	3.4	3.4	13.8	24.1	55.2	4.24	1.06
Addressing ICT Risks identified in the risk assessments contributes in enhancing the Bank's reputation and brand.	3.4	0	6.9	34.5	55.2	4.38	0.90
Addressing ICT Risks identified in the risk assessments contributes to building secure systems that increases customers confidence in the bank's systems.	3.4	0	6.9	27.6	62.1	4.45	0.91
ICT risk assessment helps to identify and quantify the risks to the organization's information assets in insider fraud prevention	3.4	0	13.8	27.6	55.2	4.31	0.97
ICT risk assessment helps the bank to register IT risks which helps in insider fraud prevention.	3.4	3.4	6.9	31.0	55.2	4.31	1.00
ICT risk assessment helps in determining the risk treatment method that leads to insider fraud prevention.	3.4	0	20.7	27.6	48.3	4.17	1.00
Aggregate score						**4.30**	**0.99**

As shown in Table 3, the aggregate mean and standard deviation are 4.30 and 0.99 respectively. The high aggregate means of 4.30 means that most of the participants strongly agreed with the statements, which represents 5 points on the Likert scale. On the other hand, the high aggregate standard deviation implies that there is a high variation in responses as shown in Table 3. In particular, the majority of participants strongly agreed that the ICT risk assessment process helps in assessing, identifying, and modifying the overall ICT risk posture to prevent insider fraud as shown by 58.6% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 24.1% of the participants rated their agreement with 4 points on the Likert scale and the other 13.8% rated their agreement with 3 points. However, 3.4% of the participants strongly disagreed that the ICT risk assessment process helps in assessing, identifying, and modifying the overall ICT risk posture to prevent insider fraud and gave it 1 point on the Likert scale.

The majority of participants strongly agreed that ICT risk assessment helps staff to have collaborate view of the entire organization from an insider fraudster perspective as shown by 48.3% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 31.0% of the participants rated their agreement with 4 points on the Likert scale and the other 17.2 % rated their agreement with 3 points. However, 3.4% of the participants strongly disagreed that ICT risk assessment helps staff to have collaborate view of the entire organization from an insider fraudster perspective and gave it 1 point on the Likert scale.

The majority of participants strongly agreed that ICT risk assessment involves identifying, evaluating, analyzing, and managing risks and thus helps prevent insider fraud as shown by 65.5% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 17.2% of the participants rated their agreement with 4 points on the Likert scale and the other 13.8 % rated their agreement with 3 points. However, 3.4% of the participants strongly disagreed that ICT risk assessment involves identifying, evaluating, analyzing, and managing risks and thus helps prevent insider fraud and gave it 1 point on the Likert scale.

The majority of participants strongly agreed that Identification of threats, vulnerabilities, risk determination, likelihood, impact analysis, and control recommendation are benefits realized from ICT risks assessment that lead to inside fraud prevention as shown by 55.2% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 20.7% of the participants rated their agreement with 4 points on the Likert scale and the other 17.2% rated their agreement with 3 points. However, 3.4% of the participants strongly disagreed that the Identification of threats, vulnerabilities, risk determination, likelihood, impact analysis, and control recommendation are benefits realized from ICT risks assessment that lead to insider fraud prevention and gave it 1 point on the Likert scale.

The majority of participants strongly agreed that Identifying the ICT risks that a Bank is facing contributes to system availability and ensures that the bank is able to provide banking services to customers as shown by 55.2% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 24.1% of the participants rated their agreement with 4 points on the Likert scale and the other 13.8% rated their agreement with 3 points. 3.4% of the participants rated their agreement with 2 points on the Likert scale. However, 3.4% of the participants strongly disagreed that Identifying the ICT risks that a Bank is facing contributes to system availability and ensures that the bank can provide banking services to customers and gave it 1 point on the Likert scale.

Most of the participants strongly agreed that addressing ICT Risks identified in the risk assessments contributes to enhancing the Bank's reputation and brand as shown by 55.2% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 34.5% of the participants rated their agreement with 4 points on the Likert scale and the other 6.9% rated their agreement with 3 points. However, 3.4% of the participants strongly disagreed that addressing ICT Risks identified in the risk assessments contributes to enhancing the Bank's reputation and brand and gave it 1 point on the Likert scale.

Most of the participants strongly agreed that addressing ICT Risks identified in the risk assessments contributes to building secure systems that increase customers' confidence in the Bank's systems as shown by 62.1% of the participants who rated the strength of their agreement

5 points on the Likert scale. On the same statements, 27.6% of the participants rated their agreement with 4 points on the Likert scale and the other 6.9% rated their agreement with 3 points. However, 3.4% of the participants strongly disagreed that addressing ICT Risks identified in the risk assessments contributes to building secure systems that increase customers' confidence in the Bank's systems and gave it 1 point on the Likert scale.

Most of the participants strongly agreed that ICT risk assessment helps to identify and quantify the risks to the organization's information assets in insider fraud prevention as shown by 55.2% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 27.6% of the participants rated their agreement their 4 points on the Likert scale and the other 13.8% rated their agreement with 3 points. However, 3.4% of the participants strongly disagreed that ICT risk assessment helps to identify and quantify the risks to the organization's information assets in insider fraud prevention and gave it 1 point on the Likert scale.

The majority of participants strongly agreed that ICT risk assessment helps the bank to register IT risks which help in insider fraud prevention as shown by 55.2% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 31.0% of the participants rated their agreement with 4 points on the Likert scale and the other 6.9% rated their agreement with 3 points. 3.4% of the participants rated their agreement with 2 points on the Likert scale. However, 3.4% of the participants strongly disagreed that ICT risk assessment helps the bank to register IT risks which help in insider fraud prevention and gave it 1 point on the Likert scale.

Finally, the majority of the participants strongly agreed that ICT risk assessment helps in determining the risk treatment method that leads to insider fraud prevention as shown by 48.3% of the participants who rated the strength of their agreement 5 points on the Likert scale. On the same statements, 27.6% of the participants rated their agreement with 4 points on the Likert scale and the other 20.7% rated their agreement with 3 points. However, 3.4% of the participants strongly disagreed that ICT risk assessment helps in determining the risk treatment method that leads to insider fraud prevention and gave it 1 point on the Likert scale.

ICT Risk Awareness

The researcher sought to establish the participant's opinion on whether ICT risk awareness has a positive influence on insider fraud in commercial banks in Nairobi County. The results are presented in figure 2 below.

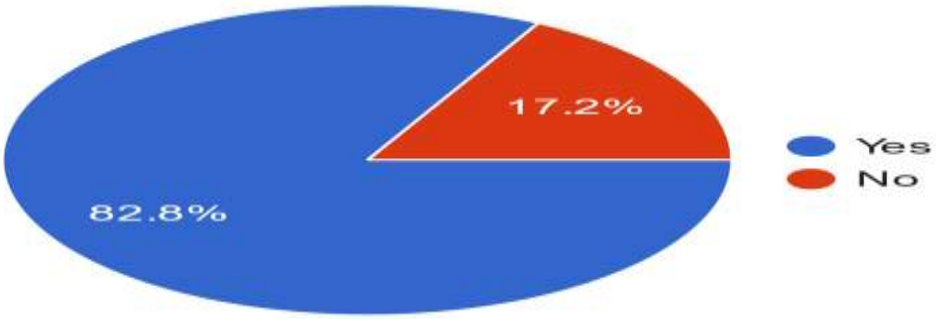

Figure 2: Respondents' Opinion on Whether ICT Risk Awareness Has a Positive Inflect on Insider Fraud

As shown in figure 2 the majority of the participants were of the opinion that ICT risk awareness has a positive inflect on insider fraud in commercial banks represented by 82.8% compared to 17.2% who were of the contrary opinion.

Further, the researcher sought to establish from the participants whose response was yes in figure 3, the extent ICT Risk awareness positively influences insider fraud. The results are presented in figure 3 below.

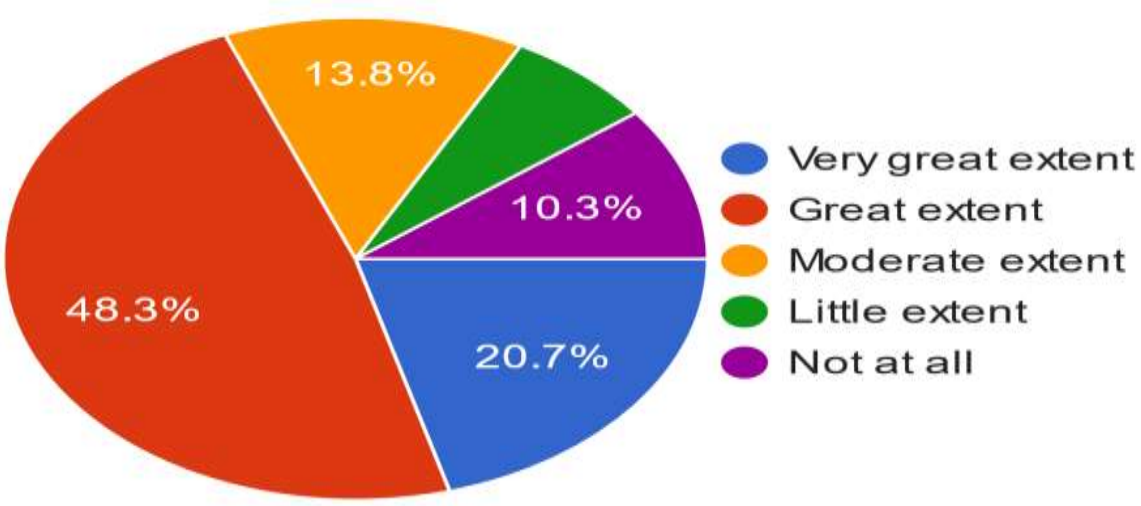

Figure 3: The Extent ICT Risk Awareness Positively Influences Insider Fraud

The results presented in figure 3 the participant's opinions varied significantly. Most of the participants were of the opinion that ICT Risk awareness positively influences insider fraud to a great extent represented by 48.3%. Those who were for a very great extent were 20.7%; those for a moderate extent were 13.8%; those who were of little extent were 6.9% and those who were for not at all were 10.3%.

Table 4: Descriptive Statistics for ICT Risk Awareness

Statements	1	2	3	4	5	Mean	Std. Dev
ICT risk awareness programs helps staff understand their responsibilities in preventing insider fraud incidences.	3.4	3.4	6.9	37.9	48.3	4.24	0.98
For ICT risk awareness to be effective banks should analyze the effect of awareness periodically.	3.4	0	6.9	27.6	62.1	4.45	0.91
Staff mandated with ICT Risk management should have the skills to identify insider fraud	3.4	0	10.3	24.1	62.1	4.41	0.95
Organizations that have ICT risk awareness programs experience less insider fraud incidents, quicker resolutions of fraud cases and enhanced customer confidence.	3.4	3.4	6.9	55.2	31.0	4.07	0.92
Employees need ICT risk awareness training since there is a greater risk of breaches occurring as a result of ignorance, inconsistent risk tolerances, or carelessness	0	3.4	0	34.5	62.1	4.55	0.69
ICT risk awareness equips staff with incident response skills that may occur due to insider fraud and prevent the bank's negative reputation	3.4	0	6.9	41.4	48.3	4.31	0.89
ICT risk awareness training provides skills and expertise that can be used to protect the bank's systems to ensure that they are available when required.	3.4	0	31.0	27.6	37.9	4.00	1.03
Aggregate score						**4.29**	**0.91**

As shown in Table 4, the aggregate means and aggregate standard deviation are 4.29 and 0.91 respectively. The high aggregate mean implies that most of the participants strongly agreed and rated their strength of agreement between 4 and 5. On the other hand, the high aggregate standard deviation shows that the variation in responses were high as shown in Table 4 above. Based on the rating on the Likert 5 points scale at 48.3%, most of the participants strongly agreed that ICT Risk awareness programs help staff understand their responsibilities in preventing insider fraud incidences. This is followed by 37.9% of the respondents who rated their agreement with the state 4 points on the Likert scale, 6.9% who rated it 3 points 3.4% who rated it 2 and finally 3.4% who strongly disagreed that ICT Risk awareness programs help staff understand their responsibilities in preventing insider fraud incidences by rating it 1 point on the Likert scale.

Most of the participants strongly agreed For ICT Risk awareness to be effective banks should analyze the effect of awareness periodically.as shown by 62.1% of the participants. This is followed by 27.6% of the respondents who rated their agreement with the statement 4 points on the Likert scale, 6.9% who rated it 3 points, and 3.4% who strongly disagreed that For ICT Risk awareness to be effective banks should analyze the effect of awareness periodically by rating it 1 point on the Likert scale.

Similarly, 62.1% of the participants strongly agreed that Staff mandated with ICT Risk management should have the skills to identify insider fraud by rating their agreement with 5 points on the Likert scale. This is followed by 24.1% of the respondents who rated their agreement with the statement 4 points on the Likert scale, 10.3% who rated it 3 points, and

3.4% who strongly disagreed that for ICT risk awareness to be effective banks should analyze the effect of awareness periodically by rating it 1 point on the Likert scale. However, 31% of the participants strongly agreed that organizations that have ICT risk awareness programs experience less insider fraud incidents, quicker resolutions of fraud cases, and enhanced customer confidence by rating the strength of their agreement 5 points on the Likert scale. On the same statement, the majority (55.2%) of the participants rated their agreement with 4 points on the Likert scale, 6.9% rated their strength 3, 3.4 rated their agreement with 2, and 3.4 % strongly disagreed and rated their strength 1 point on the Likert scale.

The majority (62.1%) of the participants strongly agreed that employees need ICT risk awareness training since there is a greater risk of breaches occurring as a result of ignorance, inconsistent risk tolerances, or carelessness by rating the strength of their agreement 5 points on the Likert scale. This is followed by 34.5% of the participants who rated their strength with 4 points; and 3.4% with 2 points on the Likert Scale. Most of the participants strongly agreed that ICT Risk awareness equips staff with incident response skills that may occur due to insider fraud and prevent the Bank's negative reputation where 48.3% rated their agreement with 5 points on the Likert scale; 41.4% rated their agreement with 4 points; 6.9% 3 points. However, 3.4% strongly disagreed that ICT Risk awareness equips staff with incident response skills that may occur due to insider fraud and prevent the Bank's negative reputation by rating their strength 1 point on the Likert scale.

Finally, most of the participants strongly agreed that ICT Risk awareness training provides skills and expertise that can be used to protect the Bank's systems to ensure that they are available when required where 37.9% of the participants rated their strength of agreed 5 points; 27.6% rated their strength 4 points, 31% rated their strength 3 points on the Likert scale. However, 3.4 % strongly disagreed that ICT Risk awareness training provides skills and expertise that can be used to protect the Bank's systems to ensure that they are available when required by rating their agreement with 1 point on the Likert scale.

Information Security Audit

The research sought to establish the extent to which participants thought that an Information Security audit influences insider fraud in commercial banks in Nairobi County. The results are presented in Table 5.

Table 5: The Extent to Which Participants' IS Audit Influences Insider Fraud

Extent	Frequency	Percentage (%)
Very great extent	9	31.0
Great extent	10	34.5
Moderate extent	7	24.1
Little extent	2	6.9
Not at all	1	3.4
Total	**29**	**100**

As shown in Table 5, the results show that 9 (31%) of the participants were of the opinion that Information Security (IS) audit influences insider fraud in commercial banks to a very great extent; 10(34.5%) to a great extent, 7(24.1%) to a moderate extent, 2 (6.9%) to a little extent, and 1 (3.4%) to no extent at all.

Table 6: Descriptive Statistics for Information Security Audit

Statements	1	2	3	4	5	Mean	Std. Dev
Information security audit helps in monitoring and measuring the efficiency and effectiveness of the Insider fraud prevention strategies.	6.9	0	17.2	24.1	51.7	4.14	1.16
To prevent insider fraud, information security audits ensures that specified management action plans remain relevant and updated.	6.9	3.4	10.3	31	48.3	4.10	1.18
Post audits reviews helps in measuring mitigation measures put in place to reduce opportunities Insider fraud prevention against the identified information security gaps.	6.9	0	10.3	37.9	44.8	4.14	1.09
Information security audit process can identify indicators that could lead to insider fraud and affect the bank's reputation.	6.9	0	10.3	34.5	48.3	4.17	1.10
Information Security audit identifies indicators that can lead to insider fraud and provide recommendations that can improve the procedures for handling customers' complaints	10.3	0	13.8	37.9	37.9	3.93	1.22
Information security audit identifies indicators that can lead to insider fraud and provide recommendations that can improve the Bank's systems availability	6.9	3.4	24.1	24.1	41.4	3.90	1.21
Information security audit helps in timely detection of fraud and therefore directly impacts the bottom line, reducing losses for an organization due to insider fraud.	10.3	13.8	17.2	20.7	37.9	3.62	1.40
Aggregate score						**4.00**	**1.19**

As summarized in Table 6, the aggregate mean and aggregate standard deviation are 4 and 1.19 respectively. The high aggregate mean of 4 shows that most of the responses were rated 4 and 5 points on the Likert scale. On the other hand, the high aggregate standard deviation of 1.19 shows there was a high variation in responses. Specifically, the majority (51.7%) of the participants strongly agreed while 6.9% strongly disagreed that an Information Security audit helps in monitoring and measuring the efficiency and effectiveness of Insider fraud prevention strategies by rating their strength of agreement with 5 points and 1 point respectively. However, 24.1% rated their strength of agreement with 4 points, and 17.2% rated their strength of agreement with 3 points on the Likert scale.

The majority (48.3%) of the participants strongly agreed while 6.9% strongly disagreed that to prevent insider fraud, Information security audits ensure that specified management action plans remain relevant and updated by rating their agreement with 5 points and 4 points respectively. On the other hand, 31% of the participants rated their agreement with 4 points; 10.3% rated 3, and 3.4% rated their agreement with 2 points on the Likert scale. Additionally, 44.8% of the participants strongly agreed and 6.9% strongly disagreed that post audits reviews

help in measuring mitigation measures put in place to reduce opportunities for insider fraud prevention by rating their agreement with 5 and 4 points respectively. However, 37.9% of the rated their agreement with 4 points, and 10.3% rated their strength with 3 points on the Likert scale.

Further, 37.9% of the participants strongly agreed and 10.3 % strongly disagreed that an Information Security audit identifies indicators that can lead to insider fraud and provide recommendations that can improve the procedures for handling customers' complaints by rating their agreement with 5 and 1 point respectively. However, 37.9% rated their agreement with 4 points, and 13.8% rated their agreement with 3 points on the Likert Scale. Additionally, 41.4% of the participants strongly agreed and 6.9% strongly disagreed that the Information Security audit identifies indicators that can lead to insider fraud and provide recommendations that can improve the Bank's systems availability by rating their agreement with 5 and 1 point respectively. However, 24.1% of the participants rated their agreement with 4 points; another 24.1% of the participants rated their agreed with 3 points, while 3.4% of the participants rated their agreement with 2 points. Finally, 37.9% strongly agreed and 10.3% strongly disagreed that an Information Security audit helps in the timely detection of fraud and therefore directly impacts the bottom line, reducing losses for an organization due to insider fraud by rating their agreement with 5 and 1 points respectively. However, 20.7% of the participants rated their agreement strength with 4 points; 17.2% with 3 points, and 13.8% with 2 points.

Information Security Policy

The researcher further sought to examine the extent the participants thought information security policy implementation influences insider fraud in commercial banks. The results are presented in Table 7.

Table 7: Extent IS Policy Implementation Influences Insider Fraud

Extent	Frequency	Percentage (%)
Very great extent	11	37.9
Great extent	12	41.4
Moderate extent	5	17.2
Little extent	1	3.4
Total	**29**	**100**

As shown in Table 7, the results show that 11 (37.9%) of the participants were of the opinion that IS policy implementation influences insider fraud in commercial banks to a very great extent; 12(41.4%) to a great extent, 5(17.2%) to a moderate extent, and 1 (3.4%) to a little extent. Further, the researcher sought to establish whether the participants had signed and read a document that states their responsibility while they are using the bank's systems. The results are presented in figure 4 below.

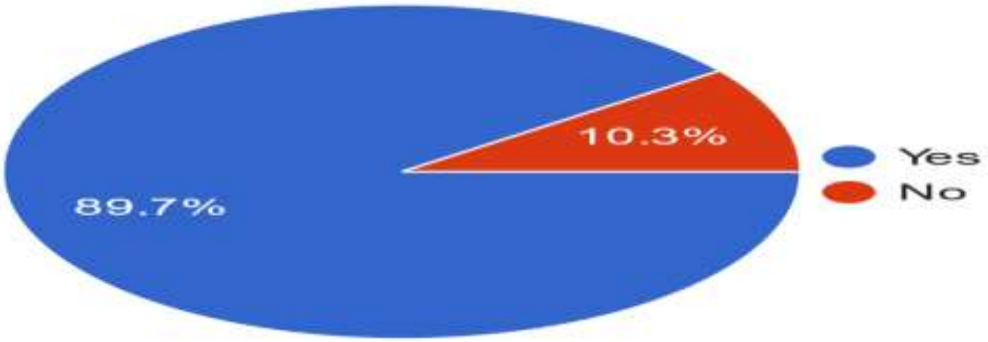

Figure 4: Whether the Participants Had Signed and Read a Document That States Their Responsibility

The results presented in figure 4 shows that the majority represented by 89.7% of the participants indicated that they had signed and read a document that states their responsibility while you are using the bank's systems. On the other hand, 10.3 % of the participants indicated that they had not signed and read a document that states their responsibility while they are using the bank's systems. Additionally, the researchers requested the participants who indicated yes above, to indicate the documents they have read and signed. The results show that the documents in included the Acceptance use policy; ICT resource Usage policy; and information and cybercrime policy.

Table 8: Descriptive Statistics for Information Security Policy

Statements	1	2	3	4	5	Mean	Std. Dev
Monitoring and reviewing staff activities against the information security policy help in reducing insider fraud incidents.	0	3.4	13.8	27.6	55.2	4.35	0.86
The information security policy allows staff members to identify an acceptable risk level and this reduces insider fraud incident.	6.9	0	20.7	37.9	34.5	3.93	1.10
Clearly communicating the information security policy implementation to all staff members reduces insider fraud incidents.	3.4	3.4	20.7	27.6	44.8	4.07	1.07
Measuring the effectiveness of the Information Security policy implementation assists banks to reduce insider fraud incidents.	0	3.4	17.2	37.9	41.4	4.17	0.85
The information security policy communicates clearly the process of handling an insider fraud incident this reduces the negative reputation that arises due to such cases.	3.4	3.4	20.7	37.9	34.5	3.97	1.02
The information security policy stipulates requirements on systems availability and as a result the Bank is able to continue to provide service to their customers	3.4	3.4	13.8	37.9	41.4	4.10	1.01
The information security policy enables Bank to implement protective measures against insider fraud which builds customers' confidence in the Bank	0	3.4	17.2	24.1	55.2	4.31	0.89
The Information Security policy communicates the measures and controls in place to prevent or reduce insider fraud.	0	6.9	24.1	24.1	44.8	4.07	0.99
Aggregate						**4.12**	**0.97**

As shown in Table 8, the aggregate mean is 4.12 and the aggregate standard deviation is 0.97. The high aggregate mean of 4.12 implies that most of the respondents strongly agreed with the statements rating their agreement with 4 or 5 points. On the other hand, the high aggregate standard deviation implies that there is a high variation in responses. Specifically, the majority of participates strongly agreed that Monitoring and reviewing staff activities against the information security policy helps in reducing insider fraud incidents and rated their agreement strength 5 points on the Likert scale. On the other hand, 27.6% of the participants rated their agreement with 4 points, 13.8% with 3 points, and 3.4% with 2 points on the Likert scale.

Further, 34.5% strongly agreed and 6.9% strongly disagreed that the information security policy allows staff members to identify an acceptable risk level and this reduces insider fraud incidents by rating their agreement with 5 and 1 point respectively. However, 37.9% rated their agreement 4 points while 20.7% rated their agreement 3 points on the Likert Scale. Additionally, 44.8% of the participants strongly agreed while 3.4 % strongly disagreed that clearly communicating the information security policy implementation to all staff members reduces insider fraud incidents by rating their agreement with 5 and 1 point respectively. On the other hand, 20.7% rated their agreement with 3 points and 3,4% with 2 points on the Likert scale.

The majority (41.4%) of the participants strongly agreed that measuring the effectiveness of the Information Security policy implementation assists banks to reduce insider fraud incidents by rating their agreement 5 points on the Likert scale. This is followed by 37.9% who rated their agreement with 4 points; 17.2% who rated their agreement with 3 points and 3.4% who rated their agreement with 2 points on the Likert scale. Additionally, 34.5% strongly agreed while 3.4% strongly disagreed that the information security policy clearly communicates the process of handling an insider fraud incident this reduces the negative reputation that arises due to such cases by rating their agreement 5 and 1 points respectively. However, 37.7 % rated their agreement with 4 points; 20.7% rated their agreement with 3 points, and 3.4% rated their agreement with 2 points.

The majority (41.4%) of the participants strongly agreed that the information security policy stipulates requirements on systems availability and as a result, the Bank is able to continue to provide service to their customers by rating their agreement 5 points on the Likert scale. On the other hand, 37.9% rated their agreement with 4 points, 13.8 % rated their agreement with 3 points, and 3.4% rated their agreement with 2 points on the Likert scale. However, 3.4 % of the participants strongly disagreed by rating their agreement with 1 point on the Likert scale.

The majority (55.2%) of the participants strongly agreed that the information security policy enables the bank to implement protective measures against insider fraud which builds customers' confidence in the Bank by rating their agreement 5 points on the Likert scale. However, 24.1% rated their agreement with 4 points; 17.2% rated their agreement with 3 points, and 3.4% rated their agreement with 2 points. Finally, the majority (44.8%) strongly agreed that the Information Security policy communicates the measures and controls in place to prevent or reduce insider fraud by rating their agreement 5 points. On the other hand, 24.1% rated their agreement 4 points, 24.1% rated their agreement 3 points, and 6.9% rated their agreement 2 points on the Likert scale.

Insider Fraud Prevention

Further, the researcher sought to establish the extent to which they think insider fraud contributes to system downtime in the bank. The results are presented in Table 12.

Table 9: The Extent to Which Insider Fraud Contributes to System Downtime

Extent	Frequency	Percentage (%)
Very great extent	4	13.8
Great extent	6	20.7
Moderate extent	11	37.9
Little extent	7	24.1
Total	**29**	**100**

As shown in Table 9, the results show that 4 (13.8%) of the participants were for the opinion that the extent to which they think insider fraud contributes to system downtime to a very great extent; 6(20.7%) to a great extent, 11 (37.9%) to a moderate extent, and 7 (24.1%) to a little extent. Further, the researcher sought to establish the percentage of information security incidents faced by their bank can be attributed to insider fraud. The results are represented in Table 10.

Table 10: Information Security Incidents Faced by the Bank Attributed to Insider Fraud

Information security incidents	Frequency	Percentage (%)
0% - 20%	14	48.3
21%-50%	2	6.9
51%-70%	10	34.5
Above 70%	3	10.3
Total	**29**	**100**

Source: Research findings, 2023

As shown in Table 10, most of the participants represented by 48.3% indicated that the percentage of information security incidents faced by their bank that can be attributed to insider fraud is between 0% to 20%, 6.9% were 21% to 50%; 34.5% were for 51% to 70%; while 10.3% were for above 70%.

Table 11: Descriptive Statistics for Insider Fraud Prevention

Statements	1	2	3	4	5	Mean	Std. Dev
ICT risk awareness has reduced in insider fraud leading to improved bank financial performances	0	0	0	41.4	58.6	4.58	0.50
ICT risk awareness has reduced insider fraud spurring confidence and trust among customers and investors	0	0	0	31.0	69.0	4.68	0.47
Information security Audit has helped commercial banks reduce insider fraud incidents	0	0	0	41.4	58.6	4.58	0.50
Information security Policy has helped commercial banks reduce financial losses due to insider fraud.	0	0	0	41.4	58.6	4.58	0.50
Aggregate						**4.60**	**0.45**

As shown in Table 11, the aggregate means and aggregate standard deviation are 4.6 and 0.45 respectively. The high aggregate mean of 4.60 implies that most of the respondents strongly agreed with the statements. On the other hand, the low mean of 0.45 implies that there is low variation in responses as shown in Table 11. Specifically, 58.6 % of the participants strongly agreed that ICT risk awareness has reduced insider fraud leading to improved bank financial performances by rating their agreement 5 points on the Likert scale. On the other hand, 41.4% of the participants rated their agreement 4 points on the Likert scale.

The participants agreed that ICT risk awareness has reduced insider fraud spurring confidence and trust among customers and investors, but the majority 69% rated their agreement 5 points while the rest 31% rated their agreement 4 points on the Likert scale. Similarly, the participants agreed that information security audit has helped commercial banks reduce insider fraud incidents with the majority, 58.6% rating their agreement 5 points and the rest 41,4% rating their agreement 4 points on the Likert scale. Finally, the participants agreed that the Information security Policy has helped commercial banks reduce financial losses due to insider fraud, with the majority of 58.6% rating their agreement 5 points while the rest 41.4% rated their agreement 4 points on the Likert Scale.

Inferential Statistics

The inferential statistics employed in this research were regression analysis and correlation analysis. The latter was utilized to investigate the association between the independent and dependent variables.

Table 12: Correlation Matrix

		Inside Fraud Prevention	ICT Assessment	ICT Awareness	IS Audit	IS Policy
Inside Fraud Prevention	Pearson Correlation	1	.253	.229	.375*	.139
	Sig. (2-tailed)		.185	.233	.045	.472
	N	29	29	29	29	29
ICT Assessment	Pearson Correlation	.253	1	.891**	.696**	.838**
	Sig. (2-tailed)	.185		.001	.001	.001
	N	29	29	29	29	29
ICT Awareness	Pearson Correlation	.229	.891**	1	.716**	.879**
	Sig. (2-tailed)	.233	.001		.001	.001
	N	29	29	29	29	29
IS Audit	Pearson Correlation	.375*	.696**	.716**	1	.718**
	Sig. (2-tailed)	.045	.001	.001		.001
	N	29	29	29	29	29
IS Ppolicy	Pearson Correlation	.139	.838**	.879**	.718**	1
	Sig. (2-tailed)	.472	.001	.001	.001	
	N	29	29	29	29	29

**. Correlation is significant at the 0.05 level (2-tailed).*

***. Correlation is significant at the 0.01 level (2-tailed).*

Correlation Analysis

The correlation between the dependent and independent variables was analyzed using Pearson's product-moment correlation coefficient (r), and the correlation matrix is presented in Table 12

As shown in Table 12, the findings reveal that the correlation between ICT risk assessment and Insider fraud prevention has a Pearson's correlation (r) = 0.253 and p-value = 0.185. Pearson's correlation of 0.253 shows a weak correlation between the ICT risk assessment and Insider fraud prevention. Additionally, the p-value of 0.185 indicates that the correlation is not statistically significant because it is more than the 0.01 and 0.05 levels of significance. This implies that there is an insignificant positive correlation between ICT risk assessment and Insider fraud prevention. As such, an increase in ICT risk assessment would cause a positive change in insider fraud prevention in commercial banks but the change would not be statistically significant. The findings show that the correlation between ICT risk awareness and Insider fraud prevention has a Pearson's correlation (r) = 0.229 and p-value = 0.233. Pearson's correlation of 0.229 shows a weak correlation between the ICT risk awareness and Insider fraud prevention. Additionally, the p-value of 0.233 indicates that the correlation is not statistically significant because it is more than the 0.01 and 0.05 levels of significance. The implication is that there is an insignificant positive correlation between ICT risk awareness and Insider fraud prevention. Thus, an increase in ICT risk awareness would cause a positive change in insider fraud prevention in commercial banks but the change would not be statistically significant.

The findings show that the correlation between information security audit and insider fraud prevention has a Pearson's correlation (r) = 0.375 and p-value = 0.045. Pearson's correlation of 0.375 shows a moderate correlation between the information security audit and Insider fraud prevention. Additionally, the p-value of 0.045 indicates that the correlation is statistically significant because it is more than the 0.05 level of significance. The implication is that there is a significant positive correlation between information security audits and Insider fraud prevention. Thus, an increase in information security audits would cause a significant positive change in insider fraud prevention in commercial banks.

Finally, the findings show that the correlation between information security policy and insider fraud prevention has a Pearson's correlation (r) = 0.139 and p-value = 0.472. Pearson's correlation of 0.139 shows a weak correlation between the information security policy and Insider fraud prevention. Additionally, the p-value of 0.472 indicates that the correlation is not statistically significant because it is more than the 0.01 and 0.05 levels of significance. The implication is that there is an insignificant positive correlation between information security policy and Insider fraud prevention. Thus, an increase in information security policy would cause a positive change in insider fraud prevention in commercial banks but the change would not be statistically significant.

Regression Analysis

The researcher also performed a multiple regression analysis to evaluate the predictive ability of the study variables. The results are presented in Table 13

Table 13: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.450[a]	.203	.070	1.77816

Predictors: (Constant), Information Security Policy, Information Security Audit, ICT risk assessment, ICT risk awareness.

As shown in Table 13, the R = 0.450, R^2 = 0.203, and adjusted R^2 = 0.070. The R-value indicates the correlation between the independent and dependent variables. The R-value represents the relationship between the dependent and independent variables. R^2 demonstrates the proportion of the dependent variable's variability explained by the independent variables. The adjusted R^2 shows the way the sample results vary from the population. As such, the results of the study show that Information Security Policy, Information Security Audit, ICT risk assessment, and ICT risk awareness contribute 20.3% of insider fraud prevention as shown by $R^{2,}$ an indication that there are other factors not studied in this research, that also determine Insider Fraud Prevention in commercial banks.

Analysis of Variance (ANOVA)

Table 14: Analysis of Variance

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	19.288	4	4.822	11.525	.027[b]
	Residual	75.885	24	3.162		
	Total	**95.172**	**28**			

a. Dependent Variable: Insider Fraud Prevention
b. Predictors: (Constant), Information Security Policy, Information Security Audit, ICT risk assessment, ICT risk awareness Source: Research findings, 2023

The results presented in Table 14 above shows that the model has a significant value of 0.027, which is less than 0.05. This implies that the model used was statistically significant to predict the way Information Security Policy, Information Security Audit, ICT risk assessment, and ICT risk awareness influence Insider Fraud Prevention. The F calculated is 11.525 as shown in table 4.17. On the other hand, the F critical at a significant level of 0.05 is 2.31, which is less that the F calculated. This confirms that the model used in the study was significant.

Coefficient of Determination

The coefficient of determination shows the significance of the independent variable and the degree to which it affects the dependent variable. The findings are presented in Table 15.

Table 15: Coefficient of Determination

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	16.351	1.851		8.833	.001
	ICT Risk Assessment	.050	.087	.239	.571	.573
	ICT Risk Awareness	.040	.159	.120	.249	.805
	IS Audit	.125	.068	.501	1.834	.079
	IS Policy	-.143	.111	-.526	-1.293	.208
A. Dependent Variable: Insider Fraud Prevention						

The results shown in Table 15 shows that ICT Risk assessment has a significant value of 0.573; ICT Risk Awareness has a significant value of 0.805; Information Security Audit has a significant value of 0.079; and Information Security has a significant value of 0.208. All the significant values for the variables are more than the acceptable significant value of 0.05 or 0.01. This means that there is no significant change of Insider Fraud Prevention as a result of the four independent variables.

The results of the coefficient of determination can also be presented using the regression equation, $\mathbf{Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon;}$

When the values are substituted in the equation, it becomes,

$\mathbf{Y} = 16.351 + \mathbf{0}.050\mathbf{X_1} + \mathbf{0}.040\mathbf{X_2} + \mathbf{0}.125\mathbf{X_3} - 0.143\mathbf{X_4} + \mathbf{1.851}$

As presented in the regression equation above, when all the independent variables (Information Security Policy, Information Security Audit, ICT risk assessment, ICT risk awareness) are held constant at zero, Insider Fraud Prevention would be 16.351, which means there would still be prevention of insider fraud. This confirms the fact that other factors determine insider fraud prevention in commercial banks. However, the prevention would not be complete without Information Security Policy, Information Security Audit, ICT risk assessment, and ICT risk awareness.

The findings further revealed that, when all the independent variables are held constant, a unit increase in ICT Risk Assessment would lead to just a 0.050 increase in Insider Fraud Prevention. A unit improvement in ICT risk awareness would cause a 0.040 increase in Insider Fraud Prevention while a unit increase in information security audit would cause a 0.125 increase in insider fraud prevention in commercial banks. Further, a unit increase in the improvement of Information security policy would cause a 0.143 decrease in insider fraud prevention in commercial banks. This shows that policy alone would not help in enhancing insider fraud prevention in commercial banks. Based on the regression equation, it is evidence that information security audit contributes more to insider fraud prevention, followed by ICT risk assessment, followed by ICT risk awareness, and finally by information security policy.

CONCLUSIONS AND RECOMMENDATIONS

The study sought to analyze the effect of ICT risk assessment on insider fraud prevention in commercial banks in Nairobi County, the findings show that ICT risk assessment has an insignificant positive effect, it is necessary for preventing insider fraud in commercial banks, but on its own, it cannot effectively prevent insider fraud. The study also sought to determine

the effect of ICT risk awareness on insider fraud prevention in Commercial Banks in Nairobi County, the findings show that it has an insignificant positive effect, it is suggested that it should be conducted among the staff members, but proper preventive measures to prevent and deter insider fraud be implemented. The study was to find out the effect of information security audits on the state of insider fraud in commercial banks in Nairobi County, the findings show that information security audit is very crucial in the prevention of insider fraud in commercial banks, it is recommended that commercial banks should have information security audits regularly but also implement other stringent measures to prevent insider fraud. The study also sought to find out the effect of information security policy implementation on the state of insider fraud in commercial banks in Nairobi County, the findings show that information security policy is essential in the prevention of insider fraud and should be put in place and all staff assisted to understand it. In conclusion, the variables studied are important but more stringent measures should be implemented in conjunction with them to effectively prevent insider fraud in commercial banks.

REFERENCES

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

ACFE. (2020). *Report to The Nations on insider fraud and abuse* https://legacy.acfe.com/report-to-the-nations/2020/docs/RTTN-Banking-Financial.pdf

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

CBK. (2017). *CBK Annual Report for 2015.* Nairobi: Central Bank Of Kenya.

CBK. (2021). Performance and Development in the Kenyan Banking Sector for the Quarter ended 31st March 2015 Retrieved from https://www.centralbank.go.ke.

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

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.

Ekran. (2021, November 23). *Insider fraud prevention: tips & tricks for your organization*. https://www.ekransystem.com/en/blog/insider-fraud-prevention.

Fraud.Net. (2019, October 31). *Internal Fraud (Insider Fraud)*. https://fraud.net/d/internal-fraud-insider-fraud/

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* . Kenya Bureau of Standards. http://www.kebs.org/index.php?opt=certification&view=isms

Ke-Cirt. (2016, January 1). About us *Communication Authority of Kenya* . Communication Authority of Kenya. http://www.ke-cirt.go.ke/index.php/about-us/

Kenyaplex. (2012, November 21) *Functions of Commercial Banks in Kenya*. Kenyaplex. https://www.kenyaplex.com/resources/6179-functions-of-commercial-banks-in-kenya.aspx

Mahinda, C. G. (2012, October). *Determinants of insider fraud in commercial banks in.* erepository.uonbi. http://erepository.uonbi.ac.ke/handle/11295/12977

Maurer, R. (2013, November 4). *Fight fraud with employee awareness*. Retrieved from www.shrm.org/hrdisciplines:http://www.shrm.org/hrdisciplines/safetysecurity/articles/pages/fight-fraud-employee-awareness.aspx

MSG. (2008, January 5). *Management study guide,expectancy theory of motivation*. Management Study Guide. http://www.managementstudyguide.com/expectancy-theory-motivation.htm

Mulwa, D. K. (2012, October). *A survey of insider information security threats in commercial banks.* Uon digital repository home. http://erepository.uonbi.ac.ke/bitstream/handle/11295/14568/Mulwa_A%20survey%20of%20insider%20information%20security%20threats%20management%20in%20commercial%20Banks%20in%20Kenya.pdf?sequence=4

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).*Uon digital repository home. 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 | IJCBSS*, 14.

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* (pp. 60-73). Perth, Western Australia: Edwin Cowan University.

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

Njiru, S. W. (2013, April 8). *A Framework to Guide Information Security Initiatives for Banking Information Systems: Kenyan Banking Sector Case Study S*trathmore university. https://su-plus.strathmore.edu/handle/11071/2336

Njuguna, M. C. (2013, October). *Response Strategies To Fraud By The Listed Commercial Banks in Kenya.* University of Nairobi repository. http://chss.uonbi.ac.ke/sites/default/files/chss/RESPONSE%20STRATEGIES%20TO%20FRAUD%20BY%20THE%20LISTED%20COMMERCIAL%20BANKS%20IN%20KENYA.pdf

Nyanchama, D. M. (2014, August 6). *Information Security in Kenya: The Missing Links.* Africa Executive.http://www.africanexecutive.com/modules/magazine/articles.php?article=7959

Omolo, S. A. (2012, June 1). *Implementation of an Information Technology Risk Management Framework;The case of Kenya Revenue Authority.* Strathmore University https://su-plus.strathmore.edu/bitstream/handle/11071/3490/Implementation.pdf?sequence=1

PWC. (2020). *2020 Global Economic Crime and Fraud Survey - Kenya report*. https://www.pwc.com/ke/en/assets/pdf/gecs-report-2020.pdf

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. doi:10.14254/2071-8330.2017/10-2/1

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*, 2178.

Scott, A. (2013, April).. *How to create a good information security policy.* Computer Weekly. https://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy

Sykes, T. A., Venkatesh, V., & Gosain, S. (2009, June 2). Model of acceptance with peer support; a social network perspective to understand employees system use. *MIS Quarterly*, pp. 371-393.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information Technology, Extending the unified theory of acceptance and use of technology. *MIS Quarterly Vol. 36 No. 1 pp. 157-178/March 2012 1*, 159.

Waitumu, N. (2014, Summer). *Upsurge of Custimers Transactions Frauds in Kenya.* United States International University Africa Digital Repository. http://erepo.usiu.ac.ke/bitstream/handle/11732/40/Njeri.pdf?sequence=1