**American Journal of Networks and Communications**
2016; 5(3): 51-59
http://www.sciencepublishinggroup.com/j/ajnc
doi: 10.11648/j.ajnc.20160503.11
ISSN: 2326-893X (Print); ISSN: 2326-8964 (Online)

**Communication**

# Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya

**Collins Odhiambo Ndalo Jowi, Elisha Abade**

School of Computing and Informatics, University of Nairobi (UON), Nairobi, Kenya

## Email address:

Collinsjowi@gmail.com (C. O. N. Jowi), eabade@uonbi.ac.ke (E. Abade)

## To cite this article:

Collins Odhiambo Ndalo Jowi, Elisha Abade. Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya. *American Journal of Networks and Communications*. Vol. 5, No. 3, 2016, pp. 51-59. doi: 10.11648/j.ajnc.20160503.11

**Received**: July 14, 2015; **Accepted**: April 5, 2016; **Published**: June 17, 2016

**Abstract:** Kenyan banks have exponentially embraced the use of information and communication technologies in their service provision. They have invested huge sums of money in implementing the self and virtual banking services with the objective of improving the quality of customer service. The study was conducted in the banking environment revealed that attaining high levels of business information integrity and overcoming users' security fears are of utmost concern. The study has also clearly established that more than coping with a technology change, a risk management strategy should address the issues related to the ethical and social areas. The study concludes that a strategy fit with appropriate, adaptable and sustainable information security solutions that addresses various social, ethical and technological issues would create a positive and secure environment that would welcome information security in banking sectors. In addition, well-formulated management strategies, security policies and data management processes that are developed with the required flexibility are the key aspects to a faultless security solution that could meet tomorrow's needs as well. In addition future studies should include the customer element to understand security issues from their viewpoint for a comprehensive information security solution in banks in Kenya.

**Keywords:** Online Banking, Online Banking Risks, IS Risk Management, IS Risk Assessment

## 1. Introduction

The banking industry is a key section in any economy and as prime movers of economic life; banks occupy a significant place in every nation. The banking sector in Kenya operates in a relatively deregulated environment. The dominance of foreign owned banks still accounts for substantial part of the banking system. Kenya's banking industry has continued to play a larger role in the country's economy compared to its neighbours.

The banking sector comprises of 45 institutions, 41 of which are commercial banks, 3 mortgage finance companies, one non-bank financial institution and one building society as at December 2006, according to CBK annual reports. However, Gulf African banks Ltd commenced banking business in November 2007 which increased them to 46 institutions by December 2007. Out of the 45 institutions, 34 are locally owned. The foreign banks comprise 6 locally incorporated and 5 branches of foreign incorporate institutions [1].

As depicted from the CBK reports, local banks dominate the Kenyan banking sector in terms of numbers, but only account for 48.2% of the sector's total assets, closely followed by the foreign owned banks with 43% of the sectors assets [2]. The Kenyan banking sector has continued to record an impressive growth in the last few years. For an example, in the period ending December 2014; the overall profitability rose by 30% while the asset portfolio expanded by 26.1%, over the previous year. The banking sector performance indicators improved with a decline in the stock of non-performing loans and enhancement of capital adequacy ratios attributed mainly to fresh capital injections and retention of profits over the same period.

The Kenyan banking industry has been expanding branch network amid the introduction of branchless banking system, which includes; use of EFTs, ATM cards, SMS banking, etc. According to annual reports from CBK, they clearly indicate that branch network has been slowly expanding since 2002. The recent introduction of robust Information Systems and

Computer Technologies has changed the face of banking worldwide. Bank managers are re-looking for better strategic options to manage their institutions amid mixed reactions from clients, regulators, governments, competitors and even critics. Organizations now totally depend on IT for better and effective communication and daily operational tasks. Advancements in IT have exposed organizations to information security threats. This research work will highlight the necessity of information security which could provide quantitative risk assessment along with the classification of risk management controls like management, operational and technical controls in organizations. It is not possible for organizations to establish information security effectively without knowing the loopholes in their controls. It is observed that mostly banks have implemented the technical and operational control appreciatively. Though, the real crux - the data security culture in organization is still a missing link in data security management. Focus will be on how Bank in Kenya evaluates and accesses the risks associated with e-Channels and more Specifically Internet Banking as an Alternative Channel.

Internet banking (e-banking) involves the use of internet and telecommunication networks to deliver a wide range of value added products and services to bank customers through the use of a system that allows individuals to perform banking activities at home or from their offices or over the internet [3]. Some online banks are traditional banks which also offer online banking, while others are online only and have no physical presence. Online banking through traditional banks enables customers to perform all routine transactions, such as account transfers, balance inquiries, bill payments, and stop-payment requests, and some even offer online loan applications. Customers can access account information at any time, day or night, and anywhere in the world. Internet banking has improved banking efficiency in rendering services to customers. Financial institutions in Kenya cannot ignore information systems since they (latter) play an important role in their operations because customers are conscious of technological advancements and demand higher quality services.

Since the inception of e-banking in Kenya, Kenyan banking institutions have witnessed many changes. Customers now have access to fast, efficient and convenient banking services. Most financial institutions in Kenya are investing large sums on money in information and communication technology (ICT). However, while the rapid development of ICT has made some banking tasks more efficient and cheaper, technological advancements have their fair share of challenges; for example they take a large share of bank resources, customer account fraud, plastic card fraud particularly on lost and stolen cards and counterfeit card fraud. Thus, there is need to manage costs and risks associated with internet banking.

It is crucial that internet banking innovations be made through sound analysis of risks and costs associated so as to avoid harm on the bank's performance. Bank performance is directly dependent on efficiency and effectiveness of internet banking and on the other hand tight controls in standards to prevent losses associated to internet banking. In order not to impair on their prosperity, financial institutions need to strike a balance between tight controls and standards in efficiency of internet banking. This is only possible if the effects of internet banking on financial institutions and its customers are well analysed and understood.

Mobile money transfer has emerged as a strong competition to banking institutions in Kenya. Initially, cellular phones were developed to improve communication from the earlier primitive forms such as smoke and drums. Later, banking institutions introduced ICT as an improvement to their banking channels. This has enabled bank customers to easily access their accounts [4]. In this regard mobile phone service providers have taken mobile money transfer services deeper into the financial sector by offering a range of financial services on their networks. Internet banking in particular is quite sensitive therefore security is central to its existence and success. The study therefore sought to find out how banks perform information risk assessment.

The study sought to the determine how banks have adopted effective and reliable security controls for electronic banking, that integrate into the bank's overall security programme, including system-wide access controls, user authentication, encryption, transaction verification, and virus protection controls; and to establish how banks have established effective risk monitoring processes, with specific emphasis on security and performance monitoring, as well as audit/quality of assurance reviews.

The study will be significant on many fronts. For instance, most Banks have institutionalized a practical risk assessment program that is important to supporting their business activities and provided several benefits.

First, and perhaps most importantly, risk assessment programs helped ensure that the greatest risks to bank operations were identified and addressed on a continuing basis. Such programs helped ensure that the expertise and best judgments of their personnel were tapped to develop reasonable steps for preventing or mitigating situations that could interfere with accomplishing the organization's mission.

Second, risk assessments helped personnel throughout the bank's better understand risks to business operations; avoid risky practices, such as disclosing passwords or other sensitive information; and be alert for suspicious events. This understanding grew, in part, from improved communication between business managers, system support staff, and security specialists.

Further, risk assessments provided a mechanism for reaching a consensus on which risks were the greatest and what steps were appropriate for mitigating them. The processes used encouraged discussion and generally required that disagreements be resolved. This, in turn, made it more likely that business managers would understand the need for agreed upon controls, feel that the controls were aligned with the banks goals, and support their effective implementation.

Finally, a formal risk assessment program provided an efficient means for communicating assessment findings and recommended actions to bank managers as well as to senior

bank officials. Standard report formats and the periodic nature of the assessments provided organizations a means of readily understanding reported information and comparing results among units over time.

# 2. Related Work

### *2.1. IS Risk Management*

Allen [5] maintained that it is unreasonable to attempt to ensure that an IS asset is 100% secure; all risks to information integrity cannot be anticipated or would cost too much in time and resources to eliminate. According to Allen, organizations must employ a risk-based approach to risk management, which is an approach that entails assessing the level of risk associated with IS assets and reducing it to an acceptable level. This risk- based approach enables an entity such as a small-sized college or university to prioritize which security practices are most important to implement to mitigate risk [6]. Allen's findings are echoed by other researchers and industry experts [7, 8, 9, 10].

In his classic work on risk management, McCumber [11] noted that experience has "taught both researchers and IT system managers that risk avoidance was simply untenable" (p. 71). Thus, McCumber emphasized the need to employ a risk-based approach to security management as opposed to risk avoidance. In arguing for a risk- based approach, Johnson, Goetz, and Pfleeger [12] stated, "Perfect security is unattainable, so the goal is risk mitigation, not risk elimination" (p. 49). Further, McCallister, Grance, and Scarfone [13] maintained that organizations of all sizes should attempt to protect information assets based on the existing level of risk rather than try to remove all risk to all IS assets. The risk-based approach entails the employment of a risk management process [14, 15]

### *2.2. Importance of IS Risk Assessment*

According to Yanosky [16], an effective risk management methodology includes conducting periodic risk assessments. As indicated in Title III of the E-Government Act of 2002 (Public Law 107-347, also known as the Federal Information Security Management Act [FISMA]), an important component of an effective information security program is the periodic completion of a risk assessment [17]. Tohidi [18] found that performing a risk assessment plays a critical role in prioritizing risks and securing IS data. Tohidi's conclusions are in keeping with the findings of Blustain, Abraham et al., [19], who maintain that performing an IS risk assessment is the foundation for an effective risk management strategy. According to Blustain, Abraham et al., [20] IS security risks must be identified by a risk assessment before these can be properly managed within an institution of higher education.

The importance of performing IS risk assessments by institutions of all sizes also is noted by Beachboard et al., [21], who stated that conducting an IS risk assessment is a key element in ensuring effective risk management. Johnson et al., [22] noted that "accurate risk assessment reduces exposure to unexpected losses and helps price risk more effectively" (p. 47). Moreover, in the latest version of the National Counterintelligence Strategy of the United States of America, the National Counterintelligence Policy Board [23] reported that assessment of human and technological vulnerabilities "is an integral part of the essential and continual task of risk management" (p. 2).

According to Ghernaouti-Helie, Simms, and Tashi [24] and Ponnam et al., [25], the main purpose of performing an effective risk assessment is to prioritize security efforts for valuable information assets, such as electronic and physical copies of student and financial information, which are vital to the continued operation of the institution. Because, for most organizations, the cost, in terms of personnel and financial resources, of mitigating all IS risks is impossible [6, 13], it is important to have a method to prioritize risk mitigation efforts. Bruijn et al., [26] asserted that one of the greatest benefits of performing a risk assessment is that the most significant threats to the institution of higher education can be identified, and cost-effective mitigation decisions that reduce risk to an acceptable level can be made. Thus, an effective risk assessment can help preserve the financial and personnel resources of an organization [27].

### *2.3. Key Elements of an IS Risk Assessment*

Researchers and practitioners have provided various descriptions of the IS risk assessment process. Generally, these investigators include three overall phases in the risk assessment process: risk identification, risk analysis, and risk evaluation [28, 29, 30]. Other well-respected researchers of risk assessment methods include a fourth phase, that of risk mitigation planning [31, 32, 33, 34, 35, 36]. This author included risk mitigation planning in the definition of the risk assessment process since risk mitigation is the immediate goal of the risk assessment process [37]. The risk identification phase includes developing an inventory of the IS assets controlled by the organization and identifying the vulnerabilities of the IS and the threats to the IS [38, 39]. Risk analysis involves determining the likelihood of the occurrence of a threat-source that successfully exploits an IS vulnerability and causes a negative impact to the organization. The risk evaluation phase involves prioritizing risks based on the most significant negative impacts that are most likely to occur. Based on these phases of the risk assessment, an organization can prioritize which IS risks need to be mitigated. The outcome of the risk assessment process is to produce a plan for mitigating IS risk to a level that is acceptable to the organization [41, 42].

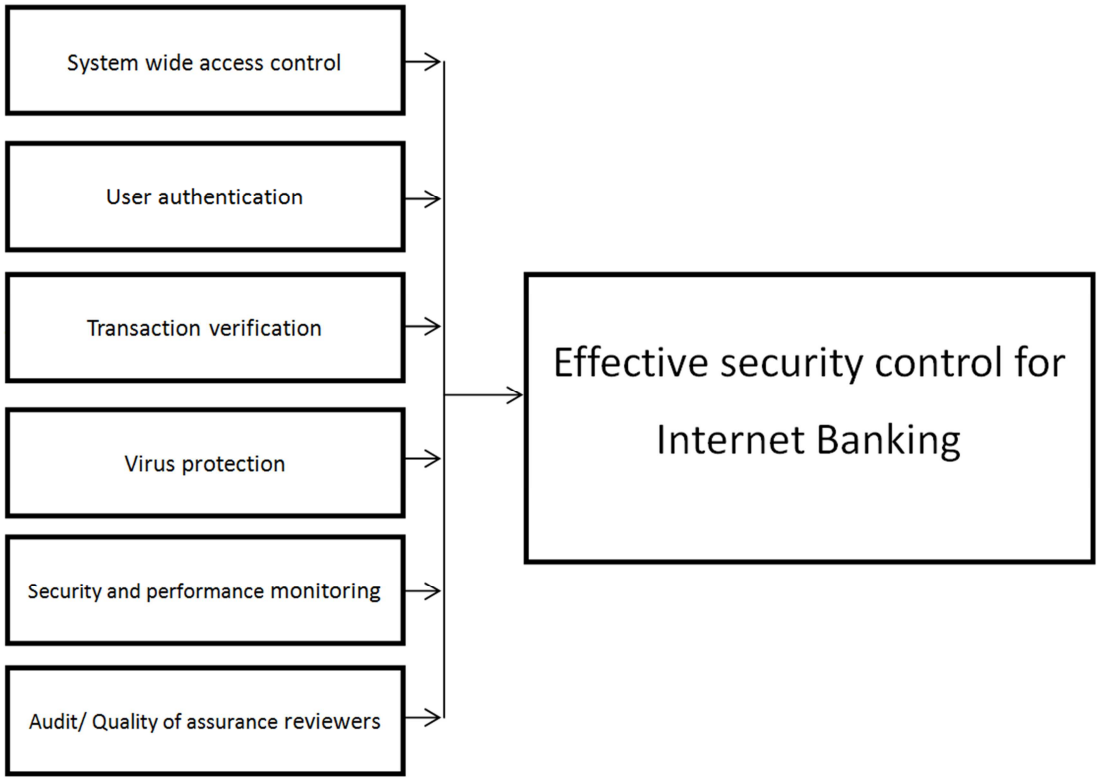
The key concepts associated with performing a risk assessment are system vulnerabilities, threats to ISs, likelihood of a threat event that compromises an IS vulnerability, impact of the security breach, risk, and risk analysis [42]. These concepts are briefly described in this section and are defined in Chapter 1. The overall risk assessment process includes identifying IS threats and vulnerabilities. A vulnerability is a potential weakness in an IS, or in the security controls for an IS, that, upon exploitation,

can result in a security breach against an entity's IS assets [43, 44]. A threat is considered a potential occurrence of an event that produces a harmful outcome to an IS, whether caused by natural events, human attackers, or system errors [37]. The agent or situation that can potentially produce the threat is known as the threat source or threat agent [37]. A threat is realized when a threat source exploits an IS vulnerability [38]

Risk is measured by a quantitative or qualitative calculation determined by the likelihood of the threat event and the impact on the organization [45, 38]. A risk analysis is the calculation of the risk, based on the identified threats and vulnerabilities of the organizations IS [27]. The likelihood of a negative event's occurring should be calculated based on the susceptibility of exploitation of the IS vulnerabilities and the ability of the threat sources to create the undesired event [37]. The impact of the threat event comprises the tangible and intangible costs to the organization that arise from the exploitation [45].

### *2.4. Own Contribution*

There are several variables that increase levels of fraud in the banking sector. Figure 1 shows those variables that contribute to the high level of internet banking insecurity in the Kenyan banking sector.




Sources: Author, 2015

***Figure 1.*** *Conceptual Framework.*

These variables are further explained the following subsections as to how they contribute towards internet banking insecurity in the Kenyan banking sector and how their relationship to effective internet banking control.

I *System wide access control*

Access is the ability to perform a function with a computer resource (e.g., use, change, or view). Access controls are the system-based means by which the ability is explicitly enabled or restricted in some way. Access controls can prescribe not only who (a user) or what (a process) is to have access to a specific system resource, but also the level of access that is permitted. Access privilege documentation must be maintained in a manner that makes it easily retrievable by individual user account. Prior to initial account distribution, positive identification of individuals receiving accounts must be conducted. Positive physical identification can be done by anyone the system administrator can trust to perform this task. For example, if an employee needs access to a system located off-site, the employee's supervisor can make positive physical identification of the employee and request access via electronic mail. During the first instance of access with a new account, the initial password must be changed by the individual responsible for the account, in compliance with the password controls defined in this policy.

II *User Authentication*

Internet banking systems must authenticate users before granting access to particular services. More precisely, the banking system must determine whether a user is, in fact, who he claims to be by asking the user to directly or indirectly prove knowledge of some sort of secret or credential. Based on the assumption that only an authentic user is able to do so, successful authentication eventually enables an authorized

user to access his private information. Expediently, all Internet banking authentication methods can be classified according to their resistance against two types of common attacks:

Offline credential stealing attacks aim at fraudulently gathering a user's credentials either by invading an insufficiently protected client PC by means of some malicious software such as a virus or trojan horse, or by tricking a user to voluntarily reveal his credentials through "phishing", that is, a combination of "spoofed" emails and mock-up web pages.

Online channel breaking attacks, such as the malicious "man-in-the-middle", the commercially motivated "market scorer" (http://www.pcworld.com/news/article/0,aid,118757,00.asp) or even the security-motivated "content inspector" (http://www.microdasys.com/), are even more sophisticated. Instead of trying to get hold of a user's credentials, messages between the client PC and the banking server are unnoticeably intercepted, the intruder masquerading as the server to the client and as the client to the server, respectively. Although the server is normally authenticated via a public-key certificate when a SSL/TLS session is established, oftentimes users are naively ignoring messages about invalid or untrusted certificates or, even worse, are fooled to trust online-generated fake server certificates from a nested intruder certification authority (CA). As a result the authenticated banking session could be hijacked or transaction data could silently be manipulated. In contrast to offline credential attacks that work decoupled from an actual user-initiated banking session, online channel breaking attacks do not necessarily compromise a user's credentials and in case require the user-initiated banking session to work on properly.

III *Transaction Verification*

As a response to the growing threats to online banking security (such as phishing and fraud) and to enhance the security, online bank systems usually implement special methods for authentication. These methods allow the authentication process at the transaction level by involving the user more in the security system having him/her confirming every transaction. User authentication alone is insufficient given the vulnerability of the standard client terminal and the relatively high risk of online bank transactions. A typical method for data origin authentication is to use an OTP (One-Time-Password) for each transaction. Another method for data origin authentication used by inline bank system is based on sending OTP with SMS message to the user's mobile phone for each financial transaction.

IV *Virus protection*

Viruses, worms, and Trojan horses are programs created by hackers that use the Internet to infect vulnerable computers. Viruses and worms can replicate themselves from computer to computer, while Trojan horses enter a computer by hiding inside an apparently legitimate program, such as a screen saver. Destructive viruses, worms, and Trojan horses can erase information from your hard disk or completely disable your computer. Others don't cause direct damage, but worsen computer's performance and stability. Antivirus programs scan e-mail and other files on your computer for viruses, worms, and Trojan horses. If one is found, the antivirus program either quarantines (isolates) it or deletes it entirely before it damages your computer and files. To protect internet banking from unauthorized transaction, virus protection must be installed and periodically updated to secure bank information from being shared with attackers and to protect uninformed customers from completing transactions.

V *Security and Performance monitoring*

While the Board of Directors has the responsibility for ensuring that appropriate security control processes are in place for e-banking, the substance of these processes needs special management attention because of the enhanced security challenges posed by e-banking. The following issues are particularly pertinent: authentication, non-repudiation, data and transaction integrity, segregation of duties, authorization controls, and maintenance of audit trails and confidentiality of key bank information.

# 3. Research Design

The study employed a descriptive research design. The choice of the design is supported by Bickman, Rog and Hedrick [46], who state that the descriptive approach is used "when the researcher is attempting to answer 'what is' or 'what was' questions".

The target population of this study consisted of all the commercial banks in Kenya with emphasis on those with branches in Nairobi. This consists of 43 banks. Thus, in total the target population was (N=43). Out of the total target population, the study targets four major departments namely; security department, operation department, audit department and risk management department.

Questionnaires were used to collect primary data from the departmental staff managers. Use of questionnaire is prompted by the fact that they are straightforward, less time consuming for both the researcher and the participants and can reach a huge sample. Questionnaires also give detailed answers to complex problems and therefore, are most effective [47].

Quantitative analysis approach was used for data analysis. Quantitative data from the questionnaires were coded and entered into the computer for computation of descriptive statistics. The Statistical Package for Social Sciences (SPSS version 20.0) was used to run descriptive analyses to produce frequency distribution and percentages.

# 4. Results and Discussions

The study found out that the majority of the respondents (94%) were male while only 6% were female indicating that most of the bank employees who work in operations and security department are male. In addition 49% of the respondents were between 30-35 years, 23% were between 36-45 years, 17% were between 26-30 years while 11% were between 51-55 years indicating that the majority of the employees were above 30 years a distribution by age bracket showing that most of those working in banking sector are youthful.

On the education levels of the respondents, the study found

out that 46% of the respondents are graduates, 29% are post graduates, 14% were diploma holders while certificate and other qualifications were 6% meaning that most of the employees who work in the bank industry have the required skills and knowledge to perform the task associated to risk management of e-banking. In addition the majority of the respondents have been working in bank sector for a period between 6-8 years as represented by 49% of the respondents. 26% have been working for 11 years and above, 14% have been working between 3-5 years while those who have been working between 1-2 years and 9-11 years were 6% respectively showing that most of the respondents have a good idea about e-banking sector and its working environment in terms of risks.

On the work departments of the respondents, the majority of the respondents were in operations department with 54%, risk management department with 40% while audit were 6% meaning that the bank sector has more staffs in operations management who keeps the bank operations at check while the majority of the respondents 46% were back office operations, 29% were managers while bank officers were 26% concluding that most of the respondents understood e-banking and risks associated with it in the bank sector.

The findings indicate that most of the respondents have knowledge about information risk management and only 6% have no idea about them indicating that information about e-banking risk management in the study will help in understanding the real risk and mitigation factors in the study while most of the institutions have risk management framework and only 6% don't have. This could be concluded to mean that most banks have risk management framework which will reduce the risk associated with e-banking

The respondents were also asked to respond to yes or no if they know threats and vulnerability with most respondents indicating they were aware about threats and vulnerability to e-banking system in the bank sector in Kenya.

On the factors that had the greatest influence on internal contributing factors, the findings indicate that failure of technology, failure of segregated duties were rated highest in influencing bank high risk management issues in e-banking in Kenya. Other variable measures that were rated highest as having the greatest influence on bank high risk management issues in e-banking were: Failure of policies and procedures, lack of training and experience, lack of internal audit, as well as lack of supervision. Agin (2006) who contended that there are many gains made by Information Technology in the management of financial services but high risk management issues in e-banking has become equally sophisticated, complex and dangerous in commercial banks through the manipulation of Information technology Systems.

***Table 1.*** *Internal factors contributing to high Risk Management issues in e-banking.*

| | Mean | Std. Deviation |
|---|---|---|
| Lack of supervision | 2.4000 | 1.53776 |
| Lack of internal audit | 2.0000 | 1.11144 |
| Failure of policies | 1.9143 | 1.29186 |
| Failure of technology | 2.4286 | 1.26690 |
| Failure of segregated duties | 2.2571 | 1.65108 |
| Lack of training | 2.0286 | 1.44478 |

On the solutions to the internal factors that contribute most to high risk management issues in e-banking, the findings indicate that that adherence to policy and procedures would reduce high risk management issues in e-banking, internal audit, the segregation of duties, staff training and risk management solutions would reduce high risk management issues in e-banking. It can be concluded that the suggested solutions have helped to reduce level of high risk management issues in e-banking in the banking sector. In addition, the study found out that internal factors can affect e-banking to a high extent. This means that internal factors do affect e-banking services if not managed and bank management has to take an initiative to control them.

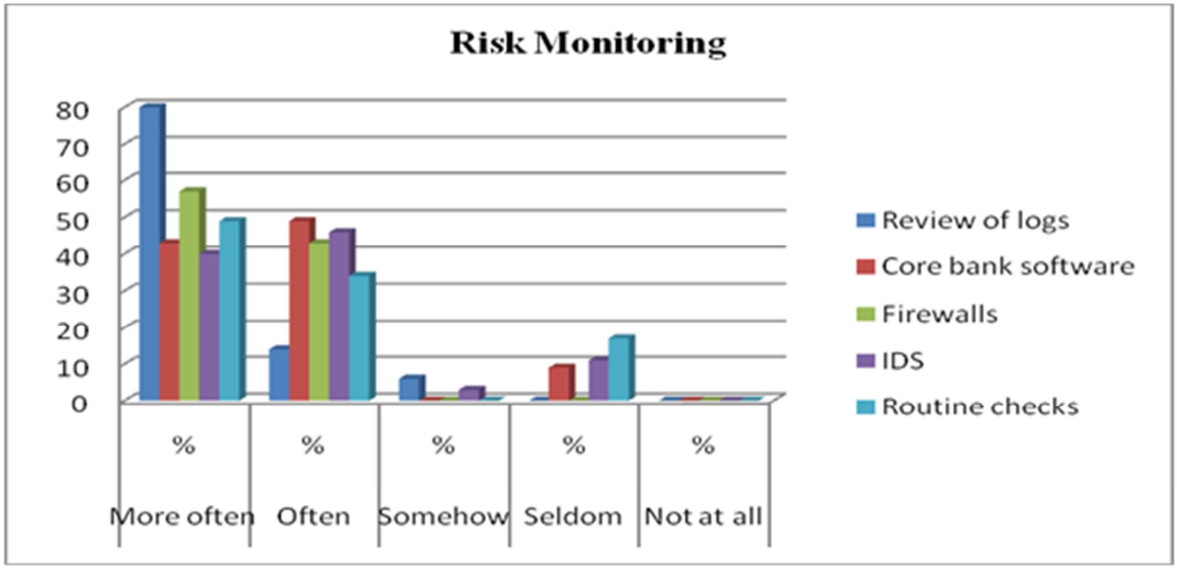



***Figure 2.*** *Risk monitoring methods.*

On the responsibility for the oversight role over risk management processes the findings indicate that senior management has the biggest oversight role over risk management process, in addition the oversight role over risk management process rest with senior management. Also designated committee was also noted as the body which has an oversight role as while the supervisory board is listed the least and not common in bank sector as shown by 3% of the respondents.

On whether banks have different types of how they audit their services to reveal any issue in their systems the findings indicates that most banks carry out internal audit as indicated by 66% of the respondents, 29% indicates that they have both audit systems (internally and externally) while 8% indicates that they carry out external audit. The findings shows that the banking sector are more concern about the services they offer and they don't take any chances of risk as all carry out auditing. In addition all the banks carry out audit after every 1-2 years as indicated by 100% of the response. This means that banks carry out audit at the end of every year to two years. This could be enough time to reduce any chances of risk in e-banking.

Accordingly review of logs, core bank softwares, firewalls, IDS and routine checks are mostly used by banks to monitor and manage risk. The most common risk monitoring method is review of logs as indicated by 80% of the respondents. This is followed by firewalls, then routine checks, core bank softwares and finally IDS. In addition the authentication procedure that is in use to validate identity of e-banking customer indicated that institutions have an authenticated procedure indicating that most of the banks are not taking any chances of risk in e-banking. Additionally the type of authentication methods being used in e-banking in validating the customer was found to be passwords, a combination of pin and password. Pin was also indicated as the most used type while only 6% indicated the use of biometrics.

***Table 2.*** *Policies and procedures in place.*

| | Mean | Std. Deviation |
|---|---|---|
| Information security Policy | 1.0000 | .00000 |
| Network security Procedures | 1.0000 | .00000 |
| Server security Procedures | 1.0571 | .23550 |
| Physical security Procedures | 1.0000 | .00000 |
| Disaster recovery Procedures | 1.0000 | .00000 |
| Backup and recovery procedures | 1.0000 | .00000 |
| Change management Procedures | 1.0000 | .00000 |
| Patch management procedures | 1.0571 | .23550 |
| Security monitoring | 1.0000 | .00000 |
| Anti-virus update procedure | 1.0000 | .00000 |

Website maintenance was also found to be one of the areas which will require attention in reducing e-banking risk with the use of the authorized staff to update or change information on the website, the update of the critical information e.g. interest rates are subjected to dual verification and the accuracy and content of website information and link to other websites, financial planning software, calculators and other interactive programs available to customers.

On the archival of times e-banking transactions, the study found out that most of the banks archived e-banking transactions being generated after every 1-3 years, 26% indicate after every 4-6 years, 11% indicate 10 years and above while 3% indicates 7-9 years meaning that majority of the e-banking transactions are being generated and archived between 1-6 years. In addition 54% of the respondents indicated that ATM surveillance are being generated and archived after every week, 37% indicate after every month, 6% indicate more than six months above while 3% indicates every six months.

To reduce risks, some policies and procedures should be in place and approved by the management. The researcher found out that most of the policies indicated were in place and only server security procedures and patch management procedures were not being used by some banks. In addition it can be summarized that integrity is the most dangerous factor in e-banking risk, Officers without enough integrity in exercising their duties would risk e-banking transactions. Greed was another factor which affects e-banking transactions. A greedy officer would in one way or another literally carry out e-banking transactions without the knowledge of the customer and this will increase risk within the bank. Lack of rewards and promotions were rated below average which could not affect e-banking transaction risk factor.

## 5. Summary and Conclusions

The study was conducted in the banking environment revealed that attaining high levels of business information integrity and overcoming users' security fears are of utmost concern. The study recommends that more than coping with a technology change, a risk management strategy in Kenyan banks should address the issues related to the ethical and social areas.

The study also recommends that a strategic fit with appropriate, adaptable and sustainable information security solutions that addresses various social, ethical and technological issues would create a positive and secure environment that would welcome information security in the Kenyan banking sector. In addition, well-formulated management strategies, security policies and data management processes that are developed with the required flexibility are the key aspects to a faultless security solution that could meet tomorrow's needs as well.

In addition future studies should include the customer element to understand security issues from their viewpoint for a comprehensive information security solution in banks in Kenya.

## Acknowledgements

First, I would like to thank the Almighty Lord for the strength and wisdom He gave me while carrying out this research project, forwithout Him, this project could not exist. I am also deeply indebted tomy supervisor Dr. Elisha Abade for

his constant guidance, positive criticism and above all his valuable suggestions and priceless advice throughout my project proposal writing, which tremendously contributed to my success within the shortest time possible.

Last but not least, Special thanks also to my family for their ever present love and support. Without them none of this would have ever happened. I hereby dedicate this piece of work to my beloved parents and my son Ryan B. O Jowi.

## References

[1] Central Bank of Kenya, Kenya Monthly Economic Review, CBK, Nairobi.

[2] Central Bank of Kenya, Historical background. Available fromhttps://www.centralbank.go.ke/index.php/component/content/article/23-deposit-protection-fundboard/134-historical-background

[3] Steven A. (2002), Information Systems: The Information of E-Business, New Jersey: Natalie Anderson, pp. 11-36

[4] Tiwari, Rajnish & Buse, Stephan & Herstatt, Cornelius, (2007). "Mobile services in banking sector: The role of innovative business solutions in generating competitive advantage," Working Papers 48, Hamburg University of Technology (TUHH), Institute for Technology and Innovation Management.

[5] Power, M. (2009). The risk management of nothing. Accounting, Organizations and Society, 34 (6–7), 849–855.

[6] Allen, J. H. (2013). Risk-centered practices. Build security in. Retrieved from https://buildsecurityin.uscert.gov/articles/bestpractices/deploymentandoperations/riskcentered-practices

[7] Ingerman, B. L., & Yang, C. (2010). Top-ten IT issues, 2010. EDUCAUSE Review, 45 (3), 46-60.

[8] Kouns, J., & Minoli, D. (2010). Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams. Hoboken, NJ: John Wiley & Sons.

[9] Landoll, D. (2011). The security risk assessment handbook: A complete guide for performing security risk assessments (2nd ed.). Boca Raton, FL: CRC Press.

[10] NIST Joint Task Force Transformation Initiative. (2011). Managing information security risk: organization, mission, and information system view: Recommendations of the National Institute of Standards and Technology (Vol. NIST Special Publication 800- 39). Gaithersburg, MD: National Institute of Standards and Technology (NIST).

[11] McCumber, J. (2005). Assessing and managing security risk in IT systems: A structured methodology. Boca Raton, FL: Auerbach.

[12] Johnson, E. M., Goetz, E., & Pfleeger, S. L. (2009). Security through information risk management. IEEE Security and Privacy, 7 (3), 45-52.

[13] McCallister, E., Grance, T., & Scarfone, K. (2009). Guide to protecting the confidentiality of personally identifiable information (PII) (Special Publication 800- 122 Draft). Gaithersburg, MD: National Institute of Standards and Technology.

[14] Kouns, J., & Minoli, D. (2010). Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams. Hoboken, NJ: John Wiley & Sons.

[15] Landoll, D. (2011). The security risk assessment handbook: A complete guide for performing security risk assessments (2nd ed.). Boca Raton, FL: CRC Press.

[16] Yanosky, R. (2007). Shelter from the storm: IT and business continuity in higher education. Boulder, CO: EDUCAUSE Center for Applied Research.

[17] NIST Joint Task Force Transformation Initiative. (2011). Managing information security risk: organization, mission, and information system view: Recommendations of the National Institute of Standards and Technology (Vol. NIST Special Publication 800- 39). Gaithersburg, MD: National Institute of Standards and Technology (NIST).

[18] Tohidi, H. (2011). The role of risk management in IT systems of organizations. Procedia Computer Science, 3, 881-887.

[19] Blustain, H., Chinniah, N., Newcomb, S., Plympton, M., & Walsh, J. (2008). Information technology and services. College and University Business Administration. National Association of Colleges and University Business Officers (NACUBO). Retrieved from http://www.nacubo.org/Products/Online_Publications/CUBA_7.html

[20] Blustain, H., Chinniah, N., Newcomb, S., Plympton, M., & Walsh, J. (2008). Information technology and services. College and University Business Administration. National Association of Colleges and University Business Officers (NACUBO). Retrieved from http://www.nacubo.org/Products/Online_Publications/CUBA_7.html

[21] Beachboard, J., Cole, A., Mellor, M., Hernandez, S., Aytes, K., & Massad, N. (2008). Improving information security risk analysis practices for small- and medium-sized enterprises: A research agenda. Issues in Informing Science and Information Technology, 5, 73-85.

[22] Johnson, E. M., Goetz, E., & Pfleeger, S. L. (2009). Security through information risk management. IEEE Security and Privacy, 7 (3), 45-52.

[23] National Counterintelligence Policy Board. (2009). The national counterintelligence strategy of the United States of America. Retrieved from http://www.ncix.gov/publications/strategy/docs/NatlCIStrategy2009.pdf

[24] Ghernaouti-Helie, S., Tashi, I., & Simms, D. (2011). Optimizing security efficiency through effective risk management. Paper presented at the International Conference on Advanced Information Networking and Applications Workshops, Biopolis, Singapore.

[25] Ponnam, A., Harrison, B., & Watson, E. (2009). Information systems risk management: An audit and control approach. In J. N. D. Gupta & S. K. Sharma (Eds.), Handbook of research on information security and assurance (pp. 68-84). Hershey, PA: Information Science Reference.

[26] Bruijn, W. D., Spruit, M. R., & van den Heuvel, M. (2010). Identifying the cost of security. Journal of Information Assurance and Security, 5, 74-83.

[27] Peltier, T. R. (2010). Information security risk analysis (3rd ed.). Boca Raton, FL: Auerbach.

[28] European Network and Information Security Agency (ENISA). (2010). ENISA emerging and future risks framework: Introductory manual. Retrieved from http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/emergingandfuture-risks-framework-introductory-manual

[29] Ghernaouti-Helie, S., Tashi, I., & Simms, D. (2011). Optimizing security efficiency through effective risk management. Paper presented at the International Conference on Advanced Information Networking and Applications Workshops, Biopolis, Singapore.

[30] Nikolic, B., & Ruzic-Dimitrijevic, L. (2009). Risk assessment of information technology systems. Issues in Informing Science and Information Technology, 6, 595-615.

[31] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the information security risk assessment process (No. CMU/SEI-2007- TR-012, ESC-TR-2007-012). Pittsburgh, PA: Software Engineering Institute: Carnegie Mellon University.

[32] Ewell, C. V. (2009, June). A method [ology] to the madness. Information Security Magazine, 21-29.

[33] Landoll, D. (2011). The security risk assessment handbook: A complete guide for performing security risk assessments (2nd ed.). Boca Raton, FL: CRC Press.

[34] McCumber, J. (2005). Assessing and managing security risk in IT systems: A structured methodology. Boca Raton, FL: Auerbach.

[35] Peltier, T. R. (2010). Information security risk analysis (3rd ed.). Boca Raton, FL: Auerbach.

[36] Syalim, A., Hori, Y., & Sakurai, K. (2009, March). Comparison of risk analysis methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. Paper presented at the 2009 International Conference on Availability, Reliability and Security, Fukuoka, Japan.

[37] NIST Joint Task Force Transformation Initiative. (2011). Managing information security risk: organization, mission, and information system view: Recommendations of the National Institute of Standards and Technology (Vol. NIST Special Publication 800- 39). Gaithersburg, MD: National Institute of Standards and Technology (NIST).

[38] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the information security risk assessment process (No. CMU/SEI-2007- TR-012, ESC-TR-2007-012). Pittsburgh, PA: Software Engineering Institute: Carnegie Mellon University.

[39] Voloudakis, J. (2006). The continuing evolution of effective IT security practices. EDUCAUSE Review, 41 (5), 30-44.

[40] Ewell, C. V. (2009, June). A method [ology] to the madness. Information Security Magazine, 21-29.

[41] Peltier, T. R. (2010). Information security risk analysis (3rd ed.). Boca Raton, FL: Auerbach.

[42] Kouns, J., & Minoli, D. (2010). Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams. Hoboken, NJ: John Wiley & Sons.

[43] European Network and Information Security Agency (ENISA). (2010). ENISA emerging and future risks framework: Introductory manual. Retrieved fromhttp://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/emergingandfuture-risks-framework-introductory-manual

[44] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). (2008). Information technology—Security techniques—Information security risk management (Vol. ISO/IEC 27005). Geneva, Switzerland

[45] Leeden, K. (2010). Security without risk? Investigating information security among Dutch universities (Master's thesis, University of Twente, Enschede, The Netherlands). Retrieved from http://purl.utwente.nl/essays/60026

[46] Mugenda, O. M & Mugenda. A. G (1999). Research methods. quantitative and qualitative approaches. (pp. 46 - 48). Nairobi, Kenya: ACTS Press.