INFORMATION SECURITY MANAGEMENT PRACTICES AND RISK EXPOSURES AMONG COMMERCIAL BANKS IN KENYA

MACHOGU, JOEL MOKAYA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE DEGREE OF MASTERS OF BUSINESS ADMINISTRATION (MBA), SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

2019

DECLARATION

This research project is my original work and has not been presented for a degree in another University

Signed: ______________________ Date: ______________________

MACHOGU J.M.

D61/6322/2017

This research project has been submitted for examination with my approval as the University Supervisor.

Signed: ______________________ Date: ______________________

JOEL K. LELEI

Department of Management Science

University of Nairobi

DEDICATION

I dedicate with love this research to my late father James Machogu Oroko for pushing and motivating me to pursue this degree and to my family who offered me unconditional love and support throughout the course of this research.

ABSTRACT

This research is about implemented information security management practices and information security risk exposures in Commercial Banks in Kenya. The research was motivated by the need to determine the extent of implementation of the information security management practices, the risk exposures as a result of not implementing the management practices and the relationship between the information security management practices and risk exposures. Commercial Banks in Kenya are facing stiff competition from FinTech companies in provision of financial services to customers and this competition has forced them to adopt technology to improve the effectiveness and efficiency of their operations, increase the customer touch points and provide services conveniently. With the huge adoption of technology to meet this needs, the organizations have in turn become more vulnerable to cyber security threats. This research therefore tries to establish to what extent commercial banks have implemented the security management practices to counter these threats. A descriptive survey targeting Information Security Managers, IT Risk Managers, IT Managers, and IT Auditors was carried out in all the 41 commercial banks in Kenya. Of the 41 respondents, 34 respondents returned fully completed survey questionnaire translating to a response rate of 82.92 percent. The survey was done using a questionnaire and descriptive statistics was used for data analysis. The study found that most organizations have implemented the information security management practices to a great extent and are exposed to information security risks to a little extent.

ACKNOWLEDGEMENTS

I would like to express my deepest appreciation to my supervisor Mr. Joel Lelei for his support, guidance and encouragement during the entire period of this research.

I would also like to thank all the academic staff in whose hands I went through, Information Security and IT Security professionals and all other personnel in the various commercial banks in Kenya who participated in this study for their co-operation; without them I wouldn’t have completed this research.

I am deeply grateful for the support my family rendered me during this time and I am forever indebted to them.

Thank you all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

The use of Information Communication Technology (ICT) in organizations has become in the recent past a key differentiator on the competitiveness of organizations. Kowalkowski, Kindström, and Gebauer (2013), assert that ICT is today used as a business enabler and that organizations that utilize ICT are deemed to have a competitive advantage. Today, ICT is not only used to support operations but also for customer acquisition, development of products, providing market intelligence, decision support, promotional activities and enhancing efficiency and effectiveness of operations.

Due to the frequent changes in the ICT industry and because ICT is a key component in facilitating the vision 2030, the Kenyan Government developed an ICT policy that provides a detailed model for legal and regulatory requirements and that enables ICT growth. The policy also promotes competitiveness in the industry while ensuring that ICT is accessible in the country. Also, it addresses matters of privacy and cybercrimes, copyright laws and intellectual property rights. This policy implementation by the Government not only indicates the criticality of ICT but also plays a key milestone in addressing the need for safe and secure use of ICT (ICT Authority, 2016).

Consequently, with the increased use of ICT to achieve these objectives, it has become increasingly necessary that organizations, customers and the Government have assurance in the secure use of ICT. The security assurance of the ICT systems is mainly focused on keeping information confidential, ensuring integrity of information and ensuring systems availability (CIA) and compliance with necessary and applicable legal, regulatory and contractual requirements. It is in this regard that organizations need to adopt ICT security best practices to ensure that the technology is not only providing the required services but also security of the technology and data is incorporated.

In the implementation of Information security practices various challenges which are multi-faceted are faced. On one hand, inadequate information security management could expose the organization to various information security challenges (risks). Non-compliance to various regulatory and contractual obligations invites fines and penalties, hacking of the bank systems by attackers leads to data integrity and confidentiality issues and system unavailability, erosion of customer confidence due to unavailability or lack of data integrity leads to lost revenue due to lost business etc.

On the other hand, there are challenges faced in the uptake of these security practices. Lack of an information security budget tops the list of challenges because the risk management activities that involve implementation of the security controls have high implementation costs. Also, outputs from the risk management exercises are often invisible and hard to justify to top management especially when there haven't been any major attacks in the organization. Senior management will tend to consider risk management a hindrance to business when the business objectives are not aligned to risk management objectives and a lack of this support will lead to non-cooperation from other stakeholders during the risk management exercises (Ernst & Young, 2014). Likewise, risk is an abstract concept and most of the times, it is expressed qualitatively. The difficulty in quantifying risk makes it hard for management to support Information security (Javaid & Iqbal, 2017).

To add to these, there are multiple standards and frameworks from which an organization can borrow best practices. Choosing a single framework or standard to use therefore is a challenge that needs to be prudently considered. However, regardless of the particular framework or standard selected for best practices adoption, managing cybersecurity is costly and requires skilled personnel, designated roles and responsibilities, top management support among other factors (Antonucci, 2017).

1.1.1 Information Security Practices

Shameli-Sendi, Aghababaei-Barzegar and Cheriet (2016) define Information Security as protecting an organization's crucial assets from alteration of critical data, disclosure of private information and disrupting critical operations. Horne, Ahmad and Maynard (2016) define a threat as an occurrence that can negatively affect an organization's business, assets or people and a vulnerability as any defectiveness in a technology system, procedures or people that exposes assets to a threat. For risk to materialize, it must be possible for a threat to take advantage of an existing defect in the system to cause harm. Risk is thus a measure of the likelihood of these threats taking advantage of the vulnerabilities and the effect this has to an organization and its stakeholders due to the operation and use of information systems. The principal means of addressing information security related risks is by the implementation of adequate and effective preventive, detective and corrective information security management practices and controls to protect these assets from compromise (Gantz & Philpott, 2012).

Some of the management practices proposed by various bodies and organizations for information security management include adequate asset management, alignment of information security objectives with business strategies, proper governance for information security, conducting regular risk assessments, ensuring there is adequate identity and access control management, facilitating information security awareness and training, ensuring there is data security, incorporating documented processes and procedures for all activities, ensuring security to organization's facilities, implementing preventive controls, continually monitoring the systems for any events, instituting proper incident management and response procedures and putting in place mechanisms to help organizations recover from disasters (International Organization for Standardization, n.d.).

1.1.2 Information Security Risk Exposures

Organizations are exposed to various information risks. Improper asset management leaves organizations vulnerable to data loss and loss of physical assets related risks. How properly and timely an organization responds to and manages an arising incident will determine its business continuity. An incident if not properly managed can be disastrous to a business. Lack of processes to guide proper provisioning and revocation of user rights leaves the information assets exposed to unauthorized access.

The growing trend for reliance on third party service providers presents attackers with new target or entry points. Organizations are widely adopting cloud computing and are transferring their data to the cloud opening up new avenues for attack. Increased regulations, laws, rules and standards related to cybersecurity from regulators only exposes organizations more and more to compliance issues as highlighted by Halibozek and Kovacich (2017).

According to Javaid and Iqbal (2017), risk is an abstract concept that is mostly expressed qualitatively. Risk is derived from the likelihood of an event occuring and the impacts given that the event occurs. Assessing the probabilities and impacts of these events is a subjective exercise. To eliminate this subjectivity, rating scales are normally used. The most commonly used scale is the Likert scale that is used to measure the attitudes, importance, likelihood etc. toward a given scenario or statement. Worth noting is that various qualitative models for measuring risk have been proposed e.g. FMEA/FMECA by reliability engineers, NIST 800-30 by NIST, CRAMM by the CCTA DREAD by Microsoft and CVSS model by First organization among others. In each of these models however, a rating scale is used to measure risk.

1.1.3 The Banking Sector in Kenya – An overview

A bank is a financial institutions licensed to receive deposits and offer loans and also provide other services e.g. exchange of foreign currency, insurance services, and safety deposit lockers among other services. They are normally classified as either commercial banks or Investment banks and they play a key role in a country’s economy. They facilitate commerce and movement of funds from savers to borrowers. They also help to enable internal and international trade by offering services like guarantees where a bank offers a guarantee on behalf of its customers, a basis upon which sellers can supply goods and services on credit. Likewise, banks create jobs by offering employment opportunities to thousands of people, 30903 as of 2017, and this helps to grow the economy since it places money in the hands of many people hence facilitating investments (Central Bank of Kenya, n.d.)

However, banks do not operate in an environment void of challenges. Banks must put processes in place to meet consistently evolving customer needs and enhance their experience. In the recent past as well, banks have experienced and are experiencing increasing competition from FinTech (Financial Technology) companies that use software to provide financial services and they have altered the way conventional banking was done. As such, they have to continually innovate and digitize their services to meet this challenge. Additionally, they face strict compliance requirements from regulatory bodies e.g. in risk management and occasionally banks have indicated that these regulations are sometimes excessive and ineffective.

In Kenya, banks are controlled by the Central Bank of Kenya. Its role is to stimulate availability of cash and ensure that these organizations can pay their debts and that they are functioning properly. It achieves these by developing laws, providing guidelines and regulations to govern the banks. They likewise license banks and ensure compliance through scrutinizing financial reports and other returns from the banks. Currently, there are forty-two commercial banks, two of which are in receivership i.e. Chase Bank Kenya and Imperial Bank Kenya (Central Bank of Kenya, 2017). Other institutions that are regulated and supervised by the Central Bank of Kenya are Microfinance Banks, Forex Bureaus and Payment Service Providers, Credit Reference Bureaus and Representative Offices of Foreign Banks. There are other financial institutions that are generally non-depository i.e. they generate funds from other sources other than deposits e.g. Mutual funds, insurance companies, pension funds, brokerage firms etc.

In their need to be competitive and to utilize technology to offer services more efficiently, banks have also inadvertently taken up cybersecurity risks. Mobile and internet banking platforms offered by banks have seen a surge in their utilization by customers. Likewise, SWIFT services that enable transfer of money in real time from one bank to another is also a widely consumed service by customers to facilitate transfer of funds internationally. Pesalink services that enable the transfer of funds to a person’s bank account utilizing mobile or internet banking applications have also seen a tremendous uptake in Kenya. Utilization of managed services by vendors and third parties expose the banks to risks related to the supply chain management. Interconnectivity between banks and Payment Service Providers e.g. Safaricom, IPSL (Integrated Payment Services Limited), etc. opens up channels through which cyber related risks emanate.

In Kenya, the October-December 2018/19 statistics released by the Communications Authority of Kenya reports that Kenya faced an increased number of cyber threats by over 10.2 million events (Communications Authority, 2019). This uptake of technology by banks leads to cybersecurity risks. It is because of this risks that this study aims to establish the controls and best practices that have been employed by banks to meet the risk exposures and to draw out the relationship between risk and best practices.

1.2 Research Problem

Today, ICT has seen huge adoption within organizations. This has seen a tremendous growth and development within banks in recent time thus spurring economic growth (Aliyu, 2019). Al-Ahmad and Mohammad (2013) illustrate how risks can be addressed by taking up standards. They note that organizations are exposed to various risks including information technology risks and they further indicate that a number of standards and frameworks and practices have been developed to aid organizations in addressing these risks. They present commonly used standards and try to identify the best selection criteria and also offer suggestions for proper implementation approaches for these best practices.

Likewise, according to Zissis and Lekkas (2012), organizations are widely adopting cloud computing. The rapid transition to cloud brings forth concerns such as information security and here they note that a number of undiscovered risks abound. To address these risks, they propose use of technological controls including cryptography and Single-Sign-On to assure integrity and confidentiality. The implementation of various security controls therefore serves to positively address risks related to information security.

In their research, Pereira, Barreto and Amaral (2017) indicate that IT has brought an important transition in organizations. This evolution has enhanced growth of cloud computing, Internet of Things, Big Data, Bring Your Own Device trends. However, these new technologies bring about security weaknesses that expose unexpected risks. Some of the major security threats as he indicates include enterprise cyber-espionage, denial-of-service and vulnerabilities within the supply chain and the extended systems.

Bouveret (2018) indicates that cyber risk has emerged as an ingrained risk concern when analyzing recent cyber incidents. The financial sector is one of the most targeted sectors because it relies heavily on information and facilitating money movement. Some of the banks that have suffered attacks in the recent past include Bank of Russia in 2016, Bangladesh Bank in 2016 where millions of dollars were stolen as well as Central Bank of Azerbaijan in 2015 where thousands of bank customer's information was stolen.

In their study, Picot, Kranz, Gupta and Ojha (2013) indicate that the increased dependence of businesses on information has created a huge requirement for information security in organizations. They further assert that technology alone cannot solve the challenges of information technology but management and behavioral aspects are just as crucial in building an information security management system. In their study they review key aspects such as support from senior management, information security training, information security culture, incident management, and compliance to regulatory requirements and conclude that security best practices have been implemented to a large extent however they propose a further study on the relationship among the information security factors.

Further, Niemimaa and Niemimaa (2017) did a study of information systems security policy implementation to try to understand how best practices were narrowed down to an organization's situational practices. They intended to understand how organizations translate best practices into their own context. They found that the adoption of the best practices to suite the individual organization context was hindered by incompatible practices, inadequate understanding of employee's roles and the information security manager not being involved in organization's business but rather allowing situational practices to guide the information security policy and actively involving staff in the rebuilding of situational practices contributed positively to the adoption of the international best practices.

On the backdrop of the fore stated studies, Makumbi, Miriti and Kahonge (2012) in their analysis found that SMEs in Kenya relied heavily on Information Technology in running business operations and therefore the risk exposed to organizations for failure in IT Security was high. They likewise found that though there was some effort to secure the IT assets, the efforts were ad hoc and that the IT security role was unallocated to someone most of the time or allocated to an individual without the requisite qualification for the role.

It is thus the reason why Disterer (2013) in his article notes that in order to protect key information assets, the standard ISO 27001 defines best practices a company can use to achieve adequate security. He further notes that with increased reliance of business processes on technology, the information and assets will be exposed to risks to a large extent keeping in mind increased levels of interconnectivity within organizations and with third parties and as such implementation of an ISMS will help prevent security breaches and risks subsequently.

Likewise, to mitigate against these risks, Ela (2011) also compares elements in various security governance frameworks, highlights their strengths and weaknesses and proposes an integrated framework that borrows practices from them. It is in light of this that this research tried to answer questions like: What are the security management practices that have been implemented in banks in Kenya? What are the key risk exposures for the banks? And what is the relationship between them?

1.3 Research Objectives

The general objectives of the study are to undertake a survey to understand what security management practices have been implemented as well as the security risks facing the Kenyan banking industry. The key objectives are to:

i. Establish the extent of implementation of Information Security Management Practices among banks in Kenya.

ii. Establish relationship between Information Security Management Practices and risk exposure among the banks in Kenya.

1.4 Value of the Study

The study is expected to help the banks in Kenya to map out their maturity level on the implementation of information security best practice. The study is also going to be an invaluable source of information to the Central Bank of Kenya because as the regulator, it is in their interest to find out how information security objectives are being met. The study is also expected to assist consultants to identify gaps in Banks that will aid them to better tailor their product and service propositions when looking for business in the Banks.

CHAPTER TWO: LITERATURE REVIEW

2.1. Introduction

This chapter covers literature guiding the study with an introduction to what Information Security Management is, a discussion on related theories to Information Security, a look at the Information Security Management Practices and a presentation of the conceptual framework.

2.2. Information Security Management

Information security management refers to the activities defined to meet the information security requirements of an organization i.e. the confidentiality of information, the integrity of the information assets and availability of the information assets (CIA Triad). To this end, identification of critical assets is done by organizations, risks and threats facing the assets are analyzed and the controls needed to counter these threats deployed. These activities are of technical, management and human nature and they involve the implementation of information security best practices (Picot et al., 2013).

Some of the top information security concerns faced by organizations worldwide include: business continuity and disaster recoverability, internal threats, access control, information security policy issues, vulnerability and risk management, malware, user security awareness i.e. training and educating users and top management support (Knapp, Marshall, Rainer Jr, & Morrow, 2006).

2.3. Theories for Information Security Management

Hong, Chi, Chao and Tang (2003) state that information security covers policies for information security, analysis of risk, planning for contingencies, management of risk and recovery from any disaster. In regards to this, various theories in relation to information security have been proposed.

The information security policy theory stipulates that to achieve information security, security policies that outline the requirements for information security have to be developed, deployed and maintained, coming to an agreement within an organization and regularly reviewing them to address the changing information security landscape (Kabay, 1996). The requirements in the policy help to ensure that all consumers of information technology comply with organization's set out objectives for securing the information and technology assets.

The theory of risk management on the other hand implores that through an enterprise-wide risk assessment, an evaluation of threats and vulnerabilities can be done. The results from the risk evaluation could then be used for prioritizing security requirements and controls with the objective of ensuring information security risk is managed (Wright, 1999). Through this analysis, threats and vulnerabilities are identified, the risks resulting from threats exploiting vulnerabilities analyzed and prioritized in terms of impacts to the business and then information security controls (best practices) implemented to counter these risks.

Management system theory proposes an information security management system (ISMS) to guide the protection of assets. The ISMS includes developing a policy, defining the scope of the ISMS, performing an assessment of risks, performing risk management by selecting controls to be implemented and preparing a document to show the controls implemented against the risk they control. An ISMS ensures the information security controls and processes are documented, internal audits are performed to ensure adequacy of controls, the controls are continually improved to address the changing environment and corrective and preventive actions undertaken to address changing risks.

In order to reduce cyber related risks, an organization can choose to institute an information security policy and ensure that all the employees adhere to the requirements defined therein. Also, an organization can perform risk analysis which will help them to classify and prioritize risk treatment options or they can implement an ISMS solution which encompasses the definition, management and continuous improvement of an information security program. All these theories in themselves articulate the management practices to be adopted to achieve information security which this research shall be studying to establish the extent of implementation of these controls.

2.4. Information Security Management Practices

Organizations draw information security best practices from a variety of bodies or organizations that have come up with standards and frameworks that define the implementation of information security controls in achieving the CIA Triad. The frequently referenced frameworks and standards for these security best practices are: PCI DSS, ISO 27001, CIS Critical Security Controls and NIST Framework. Others usually considered include COBIT and Australian Signals Directorate (ASD) Essential 8 first published in 2017 among others (NIST, 2014).

Asset Management is a key control that ensures that the critical data, people, and technology devices that enable the organization to meet its objectives are identified and documented and that processes for their management and control are properly documented, understood and implemented. These control processes should include definitions of the asset owners and ensure that users have agreed to their acceptable use (International Organization for Standardization, n.d.).

Additionally, as stated by Siponen and Willison (2009), the business environment or business alignment control requires that information on the mission and objectives of an organization is understood. The mission and objectives inform roles and responsibilities for information security, as well as decisions for risk management. In this regard, the information security objectives and strategies should be defined to support the overall business objectives and strategies. If this is not achieved, top management will start to view information security as a hindrance to business.

Likewise, as put by Ma, Johnson and Pearson (2008), the presence of proper information security policies, procedures and guidelines that help an organization to manage the regulatory, environmental, legal and operational requirements demonstrate governance controls are working. These approved documents guide the management of information security in terms of defining roles and responsibilities and assigning duties to individuals and the continued monitoring of the information security management system.

Risk Assessment as a practice on the other hand when done will identify, analyze the cybersecurity risks posed to an organization’s operations, assets and personnel. This control helps organizations to identify risks, prioritize their risk treatment plans based on criticality of these risks and to monitor that the risk has been reduced to an acceptable level. Notably, risk assessment is a continuous exercise.

Similarly, third party/vendor management as a control involves managing risks associated with third parties or vendors to ensure that the bank has established and put in place processes to identify, assess and manage risks relating to vendors and third parties as regards acquisition or outsourcing of services to third parties. The continued utilization of third party services poses risks to organizations ranging from financial, support as well as being an angle through which attackers target the organization.

To assure that access to organization's assets is limited to authorized people only and the access is managed in consistence to assessed risks, user identities should be managed and access should be controlled. Users who need access to systems need to be identified and through appropriate channels, their access granted based on need to know and least privilege basis to safeguard information assets from unauthorized access (CISECURITY, n.d.)

In other studies, it is stated, people form the weakest link in the securing of information assets. Consequently, security awareness and training for the banks staff, vendors and customers should be provided to enable them perform their duties in relation to set policies, procedures and guidelines as highlighted by Albrechtsen and Hovden (2010). Continued awareness and training reminds them of their security obligations as well as improving the security risks arising from accidental damage to information assets.

Also, an organizations data needs to be classified and labelled appropriately the information and data should be managed in congruence with an organization's data classification and risk assessment. Further, confidential data should be treated differently from public data to ensure it is not accidentally shared with unauthorized people. Additional technology solutions can be put in place to limit sharing of this data (Australian Government, 2019)

To add to these, all operational security policies should be documented alongside their supporting processes and procedures and to ensure they are used to manage protection of information assets for example backup procedures, patch management procedures, disaster recovery procedures, access management procedures etc. These procedures ensure that there is continued service delivery and that the processes are repeatable regardless of who is performing the activity.

As highlighted in the NIST framework, NIST (2014), maintenance of facilities and physical environmental security is achieved by instituting controls for ensuring there is no physical access that is granted to an organization's facilities that is not authorized. Access to data centers, offices, premises should be restricted to only authorized personnel. Additionally, movement of equipment e.g. servers, cables should be approved based on the laid down procedures on asset movement and only by authorized personnel.

An organization also needs to implement protective technical controls and that they are properly managed to ensure the security of systems and assets. E.g. Firewalls, anti-virus, Network Access Controls, etc. Other controls that can be implemented are processes and people. Some risks can only be addressed by implementing adequate technological controls e.g. scanning emails for viruses and therefore the organizations need to implement adequate technologies for this.

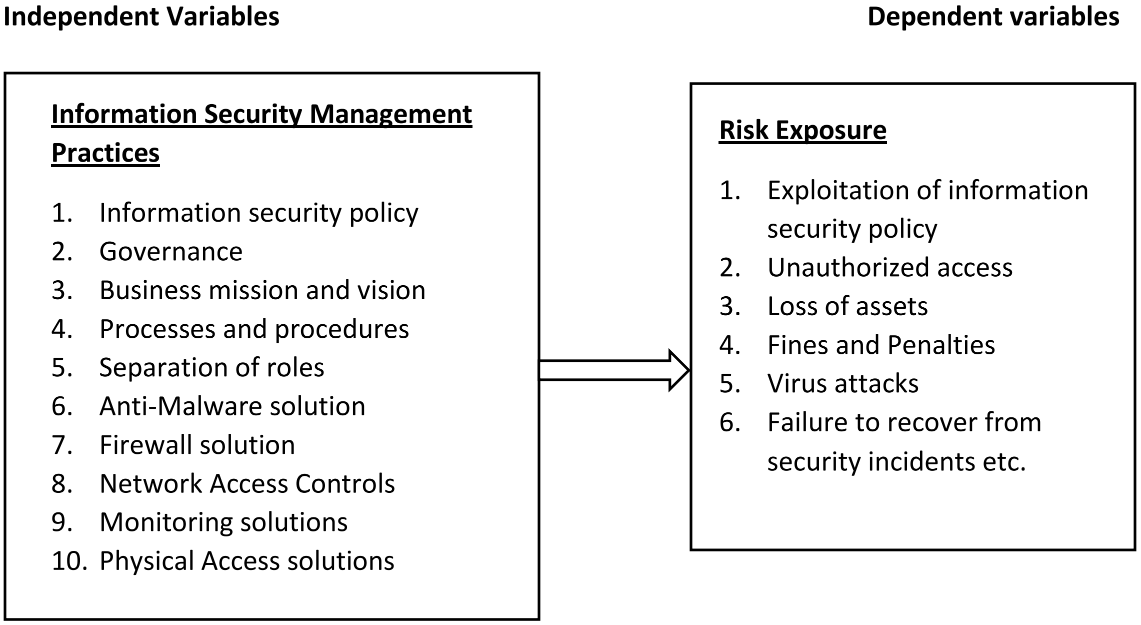
Continuous monitoring and detection of suspicious events as a control ensures that the information systems and assets are monitored to flag information security events and validate the efficacy of controls and that suspicious events are detected soon enough and addressed as per the organizations processes and procedures. In the course of system use, procedures should be put in place to monitor any exceptions or suspicious events. These exceptions are to be managed as defined in the incident management procedures.

Additionally, Werlinger, Muldner, Hawkey and Beznosov (2010) articulate that an organization's incident response management processes should be maintained, response activities coordinated with relevant partners, processes analyzed for efficacy and improvements sought by integrating lessons learnt in these response exercises. These processes define and guide how incidents/exceptions are to be raised, escalated, managed, resolved and their root causes established and permanently treated to avoid recurrence.

Information Systems Recovery determine if an organization will recover from an incident. An organization's system recovery processes should be maintained and improvements on recovery planning done by integrating lessons learnt in recovery activities and these activities should be done in conjunction with relevant parties. Occasionally, there will be a total downtime on systems. As such, processes to recover from these downtimes need to be defined and regularly tested to ensure organizations can recover from disasters.

2.5. Conceptual Framework

Horne, et al. (2016) highlight the relationships between the various components in their theory on information security as either being directional, causal etc. The theory stipulates that information security controls cause information to be protected in a positive way while threats cause information to become degraded in a negative way by degrading their integrity, confidentiality and availability. Figure 2.1 indicates the Independent Variables which are the Information Security Management Practices and how these are related to the dependent variable -risk exposure. It is clear that implementations of the Information Security Practices serve to reduce the risk exposure of the organization and their lack of serve to increase the risk exposure.



Independent Variables

Information Security Management Practices

1. Information security policy
2. Governance
3. Business mission and vision
4. Processes and procedures
5. Separation of roles
6. Anti-Malware solution
7. Firewall solution
8. Network Access Controls
9. Monitoring solutions
10. Physical Access solutions

Dependent variables

Risk Exposure

1. Exploitation of information security policy
2. Unauthorized access
3. Loss of assets
4. Fines and Penalties
5. Virus attacks
6. Failure to recover from security incidents etc.

Figure 2.1: Conceptual Model

CHAPTER THREE: RESEARCH METHODOLOGY

3.1. Research Design

This study is an exploratory survey that included all Commercial Banks in Kenya. A survey model is flexible because it enables a wide range of data to be collected. A survey enables data analysis that facilitates visualization of comparisons and generalizations between the sets of data collected.

3.2. Population

All the 41 Commercial Banks in Kenya were targeted in this study. A census approach was used with all representatives of the banks targeted.

3.3. Data Collection

Structured questionnaires were used to collect data and they were distributed to the key people familiar with the state of implementation of the information security management practices and risk exposures facing the organizations mainly in IT, Risk and Audit departments through Google forms, which they filled in online and submitted.

Section A covered the general statistics about bank including their demographic data and extent of use of ICT systems as well as capturing data about the representatives of the banks. (Respondent). Section B related to the extent of the implementation of information security management. This covered specific elements of management practice as recommended by various standards and frameworks. Section C covered the information security risks faced by the banks.

3.4. Data Analysis

Completed questionnaires were reviewed and revised for completeness before being used to facilitate data analysis. Data collected from Section A was analyzed using descriptive statistics e.g. frequency distributions, mean scores, percentages etc. to get a general look of the bank’s setup in terms of size, services etc. Data collected from Section B likewise was analyzed using descriptive statistics to identify the extent of implementation of information security best practices and factor analysis to reduce the variables to few factors. Data collected in section C was analyzed using regression analysis to determine the relationship between the best practices and risks.

The risk exposure of the organization is dependent on the information security management practices that have been implemented. This will be represented as:

$Y = a + bX_1 + cX_2 + dX_3$

Where:

Y – Denotes risk

X_1, X_2 and X_3 - these are the information security management practices

a - intercept

b, c, d – slopes

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

In this chapter are the analyzed results of the data that was collected from the respondent banks together with the discussion of the results which help to give an answer to the research questions. It represents findings on response rate, demographic information, ownership of the organization, Information Security Management Practices, Risk Exposure etc.

4.2 Response Rate

The questionnaires were mainly completed by Information Security personnel, IT Risk personnel and IT Audit personnel and ICT Managers. These individual respondents are majorly charged with managing or addressing cyber security issues in those organizations. The questionnaires were administered using Google forms to the respondents. The overall response rate was 82.92% as shown in Table 4.1. Analysis was done on individual respondent demographic data, respondent organizational data, Information Security Management Practices to determine the extent of their implementation and the information security risk exposures to determine the extent to which they are exposed and a relationship between the risk exposures and the information security management practices evaluated.

Table 4.1: Questionnaire Response Rate

Category	Percentage of responses	Response Frequency
Number of responses received	82.9%	34
Number of responses not received	17.1%	7
TOTAL DISTRIBUTED QUESTIONNAIRES		**41**

From Table 4.1, out of the 41 questionnaires sent to the 41 Commercial Banks, 34 responses were received. This translates to a response rate of 82.92%.

4.3 Demographic Information

From the respondent data summary, information on work experience, ownership structure of the bank, number of employees in the organization, the total number of customers the organization has and whether the organization utilizes cloud services or not. The respondents were mostly Business Application Managers, Information Security Managers, CISO (Chief Information Security Officer), IT Auditors, IT Managers, IT Security and IT Risk Officers.

4.3.1 Position of the Respondents

The respondents were asked to indicate the position of their role and the feedback is summarized as in Table 4.2.

Table 4.2: Position of Respondents.

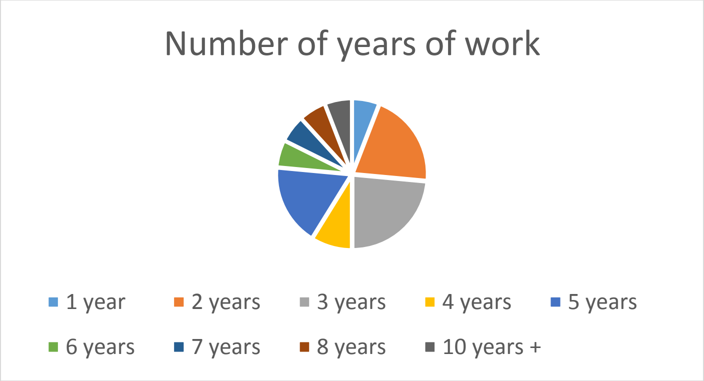
Position	**Frequency**
Business Application Manager	3
VP & Head of Operational Audits	1
CISO	1
Heads of Information Security	4
IT Security Managers	8
IT Risk Managers	4
IT Risk Officers	3
IT Security Officers	4
IT Auditor	1
IT Manager	4
IT Network Engineer	1
TOTAL	**34**

The respondents of the questionnaires were representative of the personnel who are tasked and in charge of managing the information security of the banks or giving assurance as to the state of security in the organizations and who could give a knowledgeable opinion on the state of information security in the organizations under study.

4.3.2 Duration of Work of Respondents

The respondents were asked to indicate the duration they had served in their respective roles in the organization and the feedback is summarized in Figure 4.2.

Figure 4.2: Duration of work of respondents



From Figure 4.2, 24 percent of the respondents had worked for 3 years, 21 percent for two years, and 18 percent for 5 years. 6 percent of the respondents had worked for over 10 years in their role.

4.3.3 Qualifications of Respondents

The respondents were asked to indicate their qualifications and the analyzed data is presented in Table 4.3.

Table 4.3: Respondent Education Level

Qualification	**Frequency**
Diploma	0
Undergraduate	30
Postgraduate	8
Other	9

From Table 4.3, all the respondents had undergraduate degrees with eight of them having post graduate degrees and nine of them having other certifications.

4.3.4 Ownership of the Organization

The respondents were asked to state the ownership structure of the organizations and the feedback is represented in Table 4.4.

Table 4.4: Ownership of the organization

Ownership	**Percentage**	**Frequency**
Locally owned	56%	19
Foreign owned	32%	11
Government partly owning	12%	4
TOTAL		**34**

The statistics from Table 4.4 show that 56 percent of the banks are locally owned, 32 percent foreign owned and 12 percent of them with Government partly owning them.

4.3.5 Number of Employees in the Organization

The respondents were asked to indicate the number of employees working in the organizations and the feedback is analyzed in Table 4.5.

Table 4.5: Number of employees in the organization

Number of employees	**Percentage**	**Frequency**
1 – 200	17.6%	6
201 – 500	26.4%	9
501 – 1000	20.5%	7
Over 1000	35.5%	12
Total		**34**

The results from Table 4.5 indicate that 35.5 percent of the banks have over 1000 employees with only 17 percent having less than 200 employees.

4.3.6 Number of Customers in the Organization

The respondents were asked to indicate the total number of customers that the bank serves. The results are analyzed in Table 4.6.

Table 4.6: Number of customers in the organization

Number of Customers	**Percentage**	**Frequency**
1 – 10000	8.85%	3
10001 – 100000	67.6%	23
100001 – 1000000	14.7%	5
Over 1000000	8.85%	3
TOTAL		**34**

From the feedback represented in Table 4.6, 67.6 percent of the organizations had customers between ten thousand and one hundred thousand in number with 8.85 percent having more than one million customers.

4.3.7 Extent of Bank Operations

The respondents were asked to indicate whether their organizations had operations inside and outside of Kenya and the responses are analyzed in Table 4.7.

Table 4.7: Area of bank operations

Area of bank operations	Percentage	Frequency
In and outside of Kenya	41.17%	14
Inside Kenya only	58.83%	20
TOTAL	**100%**	**34**

Statistics as shown in Table 4.7 show that 58.83 percent of banks have operations in Kenya only with 41.17 percent of the respondents indicating their banks operated in and outside Kenya.

4.3.8 Utilization of Cloud Services

The respondents were asked to indicate if they utilized cloud services in their organizational operations either as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), etc.

Table 4.8: Utilization of cloud services

Utilization of cloud services	Percentage	Frequency
Yes	85.29%	29
No	14.71%	5
TOTAL	**100%**	**34**

The feedback as represented in Table 4.8 indicates that over 85 percent of the banks utilized cloud services in their operations.

4.3.9 Organization's Duration in Operation

The respondents were asked to indicate the length of time that the bank had been in operation since inception. The feedback is analyzed in Table 4.9.

Table 4.9: Organization's duration in Operations

Duration (years)	**Percentage**	**Frequency**
Below 10	2.94%	1
10 - 20	11.76%	4
21 - 30	20.59%	7
31 - 40	23.53%	8
Over 40	41.18%	14
Total	**100%**	**34**

The results in Table 4.9 indicate that 41.18 percent of the respondent's organizations had been in operation for over 40 years and only one bank had been in operation for less than a year.

4.4 Information security Management Practices

Table 4.10: Information Security Management Practices

Answer Options	**Mean**	**Std. Deviation**
The bank has an information security policy in place that is regularly reviewed and updated in line with the technological trends in the industry.	4.264	0.609
The bank has designated roles and responsibilities for information security management and these have been allocated to individuals.	4.205	0.718
The bank has properly done segregation of duties to avoid conflict of interest.	3.676	0.830
The bank has ensured Information security has been integrated into all the projects carried out.	3.823	0.890
The bank has instituted proper policies and controls for its mobile devices e.g. laptops, USB gadgets, tablet PCs etc.	3.941	0.638
The bank has put in place mechanisms to ensure that employees and contractors are aware of the information security obligations.	4.088	0.780

The bank maintains an up to date inventory of all its assets and their ownership is defined appropriately.	3.705	0.748
The bank has properly classified and labelled its information assets and that proper security protection is accorded based on this classification.	3.529	0.977
The bank properly manages information storage media and its movement or disposal is done in a way that the contents are not compromised.	3.558	0.846
The bank has defined an adequate user access management for allocation, modification, removal/revocation of access rights and regular reviews of the access rights.	4.117	0.757
The bank has put in place appropriate system and application access control as per the access control policy e.g. password management and secure log on.	4.235	0.729
The bank has put in place cryptographic controls to secure data in transit as well as data at rest to protect it from eavesdropping and unauthorized access.	3.529	0.882
The bank has implemented physical entry controls to protect the premises, offices, data centers against unauthorized access and against environmental factors e.g. floods, earthquakes etc.	4.058	0.591
The bank has put in place mechanisms to ensure ICT equipment and its supporting utilities e.g. electric power, air conditioning, cabling are properly secured and maintained.	3.941	0.638
The bank has documented all its operating procedures and these are easily accessible, retrievable and applicable.	3.852	0.844
The bank has instituted proper change management processes to all its ICT assets.	3.764	0.769
The bank has put in place a system to monitor the capacity and performance of its networks, servers, facilities for proper management to avert incidents.	3.852	0.691

The bank has implemented comprehensive technological solutions for its key security concerns e.g. an anti-malware solution, firewalls, Multi-Factor Authentication, email filtering solution, etc.	4.147	0.732
The bank performs comprehensive backups for its systems regularly and that these backups are regularly tested to ensure the backups can be restored in the event of an incident.	4.117	0.630
The bank has mechanisms and systems in place to ensure system user and administrator activities, exceptions are logged and that the logs are adequately protected from tampering and/or deletion.	3.882	0.718
The bank has restricted permissions adequately to ensure only authorized personnel can install software on the servers and end user computers.	4.058	0.725
The bank has a vulnerability management process to ensure that technical vulnerabilities are identified, patched and continuously monitored.	3.911	0.742
The bank adequately manages its network security by employing network segmentation and limiting access to users and consultants to only those segments they need to access.	3.882	0.718
The bank has ensured that policies and procedures are defined to protect the bank's information that is accessible to third parties in the supply chain and that these are agreed within the contracts and agreements.	3.941	0.725
The bank has ensured that there are adequate Service Level Agreements defined in the contracts with third parties and these are monitored and reviewed to ensure they are met.	4.088	0.612
The bank has a robust business continuity management process and that these are regularly tested and lessons learnt properly documented for improvement.	3.823	0.821
The bank has identified and documented the set of legal,	4	0.685

regulatory and contractual obligations to which it needs to be compliant with and that these are regularly reviewed for adequacy and completeness.		
The bank carries out independent reviews of the information security management, this is reported to management, and that corrective actions are taken where appropriate.	4.088	0.658

The first objective required that we look at the extent of implementation of information security management practices among commercial banks in Kenya. A set of these practices were included in the questionnaire on a 5-point Likert scale that indicated the extent of their implementation. The Likert scale used should be interpreted as: 1 Not at all, 2 To a little extent, 3 To a moderate extent, 4 To a great extent, 5 To a very great extent. The means and standard deviations are to be interpreted according to this scale. From the data in Table 4.10, it can be inferred that the below information security management practices have been implemented. The mean values calculated can be rounded off to the nearest whole number and then interpreted using the Likert scale used.

The bank has put in place mechanisms to ensure that employees and contractors are aware of the information security obligations (mean of 4.088 and standard deviation of 0.780). The bank has an information security policy in place that is regularly reviewed and updated in line with the technological trends in the industry (mean of 4.264 and standard deviation of 0.609). The bank has designated roles and responsibilities for information security management and these have been allocated to individuals (mean of 4.205 and standard deviation of 0.718). The bank has properly done segregation of duties to avoid conflict of interest (mean of 3.676 and standard deviation of 0.830).

The bank has ensured Information security has been integrated into all the projects carried out (mean of 3.823 and standard deviation of 0.890). The bank has instituted proper policies and controls for its mobile devices e.g. laptops, USB gadgets, tablet PCs etc. (mean of 3.941 and standard deviation of 0.638). The bank maintains an up to date inventory of all its assets and their ownership is defined appropriately (mean of 3.705 and standard deviation 0.748). The bank has properly classified and labelled its information assets and that proper security protection is accorded based on this classification (mean of 3.529 and standard deviation 0.977). The bank properly manages information storage media and its movement or disposal is done in a way that the contents are not compromised (mean of 3.558 and standard deviation 0.846). The bank has defined an adequate user access management for allocation, modification, removal/revocation of access rights and regular reviews of the access rights (mean of 4.117 and standard deviation of 0.757).

The bank has put in place mechanisms to ensure ICT equipment and its supporting utilities e.g. electric power, air conditioning, cabling are properly secured and maintained (mean of 3.941 and standard deviation 0.638). The bank has documented all its operating procedures and these are easily accessible, retrievable and applicable (mean of 3.852 and standard deviation of 0.844). The bank has instituted proper change management processes to all its ICT assets (mean of 3.764 and standard deviation of 0.769). The bank performs comprehensive backups for its systems regularly and that these backups are regularly tested to ensure the backups can be restored in the event of an incident (mean of 4.117 and standard deviation of 0.630). The bank has ensured that policies and procedures are defined to protect the bank’s information that is accessible to third parties in the supply chain and that these are agreed within the contracts and agreements (mean of 3.941 and standard deviation of 0.725).

The bank has ensured that there are adequate Service Level Agreements defined in the contracts with third parties and these are monitored and reviewed to ensure they are met (mean of 4.088 and standard deviation of 0.612). The bank has a robust business continuity management process and that these are regularly tested and lessons learnt properly documented for improvement (mean of 3.823 and standard deviation of 0.821). The bank has identified and documented the set of legal, regulatory and contractual obligations to which it needs to be compliant with and that these are regularly reviewed for adequacy and completeness (mean of 4.0 and standard deviation of 0.685). The bank carries out independent reviews of the information security management and this is reported to management and that corrective actions are taken where appropriate (mean of 4.088 and standard deviation of 0.658)

The bank has put in place appropriate system and application access control as per the access control policy e.g. password management and secure log on (mean of 4.235 and standard deviation of 0.729). The bank has put in place cryptographic controls to secure data in transit as well as data at rest to protect it from eavesdropping and unauthorized access (mean of 3.529 and standard deviation of 0.882). The bank has implemented physical entry controls to protect the premises, offices, data centers against unauthorized access and against environmental factors e.g. floods, earthquakes etc. (mean of 4.058 and standard deviation of 0.591). The bank has put in place a system to monitor the capacity and performance of its networks, servers, facilities for proper management to avert incidents (mean of 3.852 and standard deviation of 0.691). The bank has implemented comprehensive technological solutions for its key security concerns e.g. an anti-malware solution, firewalls, Multi-Factor Authentication, email filtering solution, etc. (mean of 4.147 and standard deviation of 0.732).

The bank has mechanisms and systems in place to ensure system user and administrator activities, exceptions are logged and that the logs are adequately protected from tampering and/or deletion (mean of 3.882 and standard deviation of 0.718). The bank has restricted permissions adequately to ensure only authorized personnel can install software on the servers and end user computers (mean of 4.058 and standard deviation of 0.725). The bank has a vulnerability management process to ensure that technical vulnerabilities are identified, patched and continuously monitored (mean of 3.911 and standard deviation of 0.742). The bank adequately manages its network security by employing network segmentation and limiting access to users and consultants to only those segments they need to access (mean of 3.882 and standard deviation of 0.718).

Given the number of variables, factor analysis was done. Factor analysis is a technique used to reduce a large number of variables into fewer numbers of factors. This effectively extracts maximum common variance from all variables and puts them into a common score. In our case, 28 variables were reduced into five factors. The analysis of the factor analysis is presented in the following tables.

Table 4.11: Total Variance

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	15.458	55.207	55.207	15.458	55.207	55.207	6.023	21.511	21.511
2	1.737	6.204	61.411	1.737	6.204	61.411	4.430	15.822	37.333
3	1.617	5.773	67.185	1.617	5.773	67.185	3.782	13.507	50.840
4	1.261	4.504	71.688	1.261	4.504	71.688	3.478	12.423	63.263
5	1.115	3.980	75.669	1.115	3.980	75.669	3.474	12.406	75.669
6	.970	3.465	79.134						
7	.788	2.816	81.949						
8	.658	2.351	84.300						
9	.629	2.247	86.547						
10	.567	2.026	88.573						
11	.494	1.764	90.337						
12	.445	1.590	91.927						
13	.422	1.507	93.434						
14	.324	1.156	94.590						
15	.297	1.061	95.651						
16	.245	.877	96.528						
17	.215	.766	97.294						
18	.156	.556	97.850						
19	.146	.521	98.371						
20	.116	.414	98.785						
21	.098	.349	99.133						
22	.079	.283	99.416						
23	.060	.214	99.631						
24	.049	.175	99.805						
25	.029	.103	99.908						
26	.014	.049	99.957						
27	.007	.026	99.983						
28	.005	.017	100.000						

From Table 4.11, five factors account for 75.67 percent of the variance. Notably, variable one (The bank has an information security policy in place that is regularly reviewed and updated in line with the technological trends in the industry.) accounts for 15.45 of the total variance.

Table 4.12: Rotated Component Matrix

Rotated Component Matrix					
	Component				
	1	2	3	4	5
The bank has an information security policy in place that is regularly reviewed and updated in line with the technological trends in the industry.	.185	.051	.742	.371	-.014
The bank has designated roles and responsibilities for information security management and these have been allocated to individuals.	.657	.336	.131	.320	.241
The bank has properly done segregation of duties to avoid conflict of interest.	.848	.310	.230	.106	.020
The bank has ensured Information security has been integrated into all the projects carried out.	.705	.160	.221	.202	.247
The bank has instituted proper policies and controls for its mobile devices e.g. laptops, USB gadgets, tablet PCs etc.	.521	.030	.271	.532	.397

The bank has put in place mechanisms to ensure that employees and contractors are aware of the information security obligations.	.683	.025	.288	.381	.027
The bank maintains an up to date inventory of all its assets and their ownership is defined appropriately.	.288	.442	.611	.284	.080
The bank has properly classified and labelled its information assets and that proper security protection is accorded based on this classification.	.443	.444	-.013	.546	.219
The bank properly manages information storage media and its movement or disposal is done in a way that the contents are not compromised.	.399	.120	.231	.730	.323
The bank has defined an adequate user access management for allocation, modification, removal/revocation of access rights and regular reviews of the access rights.	.618	.288	.136	.403	.238

The bank has put in place appropriate system and application access control as per the access control policy e.g. password management and secure log on.	.478	.108	.696	.047	.264
The bank has put in place cryptographic controls to secure data in transit as well as data at rest to protect it from eavesdropping and unauthorized access.	.402	.639	-.062	.402	.362
The bank has implemented physical entry controls to protect the premises, offices, data centers against unauthorized access and against environmental factors e.g. floods, earthquakes etc.	.264	.116	.635	-.014	.330
The bank has put in place mechanisms to ensure ICT equipment and its supporting utilities e.g. electric power, air conditioning, cabling are properly secured and maintained.	.459	-.015	.269	.126	.731
The bank has documented all its operating procedures and these are easily accessible, retrievable and applicable.	.374	.713	.274	.215	.052

The bank has instituted proper change management processes to all its ICT assets.	.603	.544	.272	.291	.212
The bank has put in place a system to monitor the capacity and performance of its networks, servers, facilities for proper management to avert incidents.	.441	.450	.203	.011	.431
The bank has implemented comprehensive technological solutions for its key security concerns e.g. an anti-malware solution, firewalls, Multi-Factor Authentication, email filtering solution, etc.	.504	.281	.267	.378	.314
The bank performs comprehensive backups for its systems regularly and that these backups are regularly tested to ensure the backups can be restored in the event of an incident.	-.005	.296	.654	.131	.315
The bank has mechanisms and systems in place to ensure system user and administrator activities, exceptions are logged and that the logs are adequately protected from tampering and/or deletion.	.319	.538	.531	.069	.408

The bank has restricted permissions adequately to ensure only authorized personnel can install software on the servers and end user computers.	.141	.874	.259	.074	.095
The bank has a vulnerability management process to ensure that technical vulnerabilities are identified, patched and continuously monitored.	.518	.419	.409	.162	.382
The bank adequately manages its network security by employing network segmentation and limiting access to users and consultants to only those segments they need to access.	.019	.612	.111	.621	.217
The bank has ensured that policies and procedures are defined to protect the bank’s information that is accessible to third parties in the supply chain and that these are agreed within the contracts and agreements.	.240	.244	.350	.379	.605

The bank has ensured that there are adequate Service Level Agreements defined in the contracts with third parties and these are monitored and reviewed to ensure they are met.	.026	.284	.218	.303	.745
The bank has a robust business continuity management process and that these are regularly tested and lessons learnt properly documented for improvement.	.396	.469	.122	.373	.420
The bank has identified and documented the set of legal, regulatory and contractual obligations to which it needs to be compliant with and that these are regularly reviewed for adequacy and completeness.	.357	.247	.328	.635	.077
The bank carries out independent reviews of the information security management and this is reported to management and that corrective actions are taken where appropriate.	.652	.266	.195	.117	.482

From Table 4.12, the first factor is highly correlated with eight variables which are: The bank has designated roles and responsibilities for information security management and these have been allocated to individuals. In addition, the bank has properly done segregation of duties to avoid conflict of interest. Additionally, the bank has ensured Information Security has been integrated into all the projects carried out. In addition, the bank has put in place mechanisms to ensure that employees and contractors are aware of the information security obligations. The bank has also defined an adequate user access management for allocation, modification, removal/revocation of access rights and regular reviews of the access rights. Additionally, the bank has implemented comprehensive technological solutions for its key security concerns e.g. an anti-malware solution, firewalls, Multi-Factor Authentication, email filtering solution, etc. In addition, the bank has a vulnerability management process to ensure that technical vulnerabilities are identified, patched and continuously monitored, the bank carries out independent reviews of the information security management, this is reported to management, and that corrective actions are taken where appropriate.

The second factor is highly correlated with three variables which are: The bank has put in place cryptographic controls to secure data in transit as well as data at rest to protect it from eavesdropping and unauthorized access. In addition, the bank has documented all its operating procedures and these are easily accessible, retrievable and applicable. Likewise, the bank has restricted permissions adequately to ensure only authorized personnel can install software on the servers and end user computers.

The third factor is highly correlated with five variables, which are: The bank has an information security policy in place that is regularly reviewed and updated in line with the technological trends in the industry. In addition, the bank maintains an up to date inventory of all its assets and their ownership is defined appropriately. Likewise, the bank has put in place appropriate system and application access control as per the access control policy e.g. password management and secure log on. The bank has also implemented physical entry controls to protect the premises, offices, data centers against unauthorized access and against environmental factors e.g. floods, earthquakes etc. In addition, the bank performs comprehensive backups for its systems regularly and that these backups are regularly tested to ensure the backups can be restored in the event of an incident.

The fourth factor is highly correlated with three variables which are: The bank has properly classified and labelled its information assets and that proper security protection is accorded based on this classification. In addition, the bank properly manages information storage media and its movement or disposal is done in a way that the contents are not compromised. Likewise, the bank has identified and documented the set of legal, regulatory and contractual obligations to which it needs to be compliant with and that these are regularly reviewed for adequacy and completeness.

The fifth factor is also highly correlated with three factors which are: The bank has put in place mechanisms to ensure ICT equipment and its supporting utilities e.g. electric power, air conditioning, cabling are properly secured and maintained. In addition, the bank has ensured that policies and procedures are defined to protect the bank's information that is accessible to third parties in the supply chain and that these are agreed within the contracts and agreements. Likewise, the bank has ensured that there are adequate Service Level Agreements defined in the contracts with third parties and these are monitored and reviewed to ensure they are met.

These variables are thereafter used for the regression analysis to determine the relationship between the dependent and independent variables.

4.5 Information Security Risk Exposures

Likewise, a set of these risks were included in the questionnaire on a 5-point Likert scale to determine the extent of their prevalence in the organizations. The Likert scale used should be interpreted as: 1 Not at all, 2 To a little extent, 3 To a moderate extent, 4 To a great extent, 5 To a very great extent. The means and standard deviations are to be interpreted according to this scale. From the data in Table 4.13, it can be inferred that the below information security risk exposures are prevalent. The mean values calculated can be rounded off to the nearest whole number and then interpreted based on the Likert scale.

There are risks arising from intentional or accidental exploitation of specific information security clauses/requirements that have not been defined in the existing information security policy (mean of 1.970 and standard deviation of 0.617). Risks of uncoordinated information security management because there are no clear roles and responsibilities for information security defined and assigned to individuals (mean of 1.941 and standard deviation of 0.683). Risk of inappropriate and unauthorized activities perpetrated by individuals intentionally or accidentally because of conflicting roles and areas of responsibility (mean of 2.352 and standard deviation of 0.680). Risk of systems being commissioned with security vulnerabilities because information security requirements were not incorporated into the project life cycle (mean of 2.117 and standard deviation of 0.675). Reputational and legal risks arising from inadequate management of mobile devices (mean of 2.058 and standard deviation of 0.683). Risk of breach of the requirements of the information security policy by staff and contractors due to lack of awareness creation and training making them unaware of their obligations to security (mean of 1.911 and standard deviation of 0.701).

There also exists risks of loss of assets or introduction of malicious assets in the network arising from inadequate asset/inventory management (mean of 2.117 and standard deviation of 0.718). Legal and reputational risk arising from leakage of sensitive and confidential information to unauthorized people (mean of 2.088 and standard deviation of 0.612). Risks arising from intentional or accidental manipulation of data due to excessive access rights provisioned to users coupled with lack of regular access rights reviews (mean of 2.029 and standard deviation of 0.568). Risks of unauthorized and uncontrolled access to banks application systems due to inadequate access controls e.g. passwords, 2FA etc. (mean of 1.882 and standard deviation of 0.582). Risk of data loss/theft that is in transit or at rest due to improper application of encryption controls (mean of 2.529 and standard deviation of 0.737).

In addition, there are risks of unauthorized access to the banks premises, offices and data centers due to inadequate physical entry controls (mean of 1.882 and standard deviation of 0.403). Risk of loss of assets due to inappropriate controls for removal of ICT equipment from the bank’s premises (mean of 1.764 and standard deviation of 0.545).

Risks of prolonged system outages because of lack of documented operating procedures that are easily accessible and easy to follow (mean of 2.205 and standard deviation of 0.631). Risk of system unavailability and unauthorized changes to bank systems because of absence of change management procedures or lack of adherence to them (mean of 1.941 and standard deviation of 0.591). Risk of system unavailability occasioned by lack of resource monitoring for capacity and performance (mean of 2.147 and standard deviation of 0.6). Risk of hacking attacks on organization assets due to lack of implementation of appropriate and comprehensive technology controls e.g. anti-virus solution, firewalls, email gateways etc. (mean of 2.205 and standard deviation of 0.676).

There are risks of a bank's inability to recover from a security incident due to inability to restore backups since these backups are not frequently and adequately tested (mean of 1.852 and standard deviation of 0.647). Risk of inability of the bank to monitor, analyze security incident and conduct forensic investigations due to lack of system event logs or due to audit logs that have been tampered with due to inadequate protection (mean of 2.235 and standard deviation of 0.688). Risk of malicious software installations that could lead to unauthorized access to or modification of information assets due to unauthorized users having permissions to install software on computers (mean of 2.029 and standard deviation of 0.568). Risks of proliferation of vulnerabilities that expose the systems to exploitation due to lack of adequate vulnerability management and patching of vulnerable systems (mean of 2.088 and standard deviation of 0.612).

There are also risks arising from a lack of necessary and adequate contractual clauses in contracts signed with third parties that indemnify the bank in the event certain agreements are breached by vendors (mean of two and standard deviation of 0.485). Risks of fines and penalties from regulators and contractors breaching contractual terms (mean of 1.970 and standard deviation of 0.513). Risks of inability of the bank to recover from a disaster due to untested disaster recovery and business continuity plans (mean of 1.970 and standard deviation of 0.452).

Table 4.13: Information Security Risk Exposures

Answer Options	Mean	Std. Deviation
Intentional or accidental exploitation of specific information security clauses/requirements that have not been defined in the existing information security policy.	1.970	0.617
Uncoordinated information security management because there are no clear roles and responsibilities for information security defined and assigned to individuals.	1.941	0.683
Inappropriate and unauthorized activities perpetrated by individuals intentionally or accidentally because of conflicting roles and areas of responsibility.	2.352	0.680
Systems are commissioned with security vulnerabilities because information security requirements were not incorporated into the project life cycle.	2.117	0.675
Reputational and legal risks arising from inadequate management of mobile devices.	2.058	0.683
Breach of the requirements of the information security policy by staff and contractors due to lack of awareness creation and training making them unaware of their obligations to security.	1.911	0.701
Loss of assets or introduction of malicious assets in the network arising from inadequate asset/inventory management.	2.117	0.718
Legal and reputational risk arising from leakage of sensitive and confidential information to unauthorized people.	2.088	0.612
Intentional or accidental manipulation of data due to excessive access rights provisioned to users coupled with lack of regular access rights reviews.	2.029	0.568
Unauthorized and uncontrolled access to banks application systems due to inadequate access controls e.g. passwords, 2FA etc.	1.882	0.582

Data loss/theft that is in transit or at rest due to improper application of encryption controls.	2.529	0.737
Data loss/theft that is in transit or at rest due to improper application of encryption controls.	2.588	0.691
Unauthorized access to the banks premises, offices and data centers due to inadequate physical entry controls.	1.882	0.403
Loss of assets due to inappropriate controls for removal of ICT equipment from the bank’s premises.	1.764	0.545
Prolonged system outages because of lack of documented operating procedures that are easily accessible and easy to follow.	2.205	0.631
System unavailability and unauthorized changes to bank systems because of absence of change management procedures or lack of adherence to them.	1.941	0.591
System unavailability occasioned by lack of resource monitoring for capacity and performance.	2.147	0.600
Hacking attacks on organization assets due to lack of implementation of appropriate and comprehensive technology controls e.g. anti-virus solution, firewalls, email gateways etc.	2.205	0.676
Inability to recover from a security incident due to inability to restore backups since these backups are not frequently and adequately tested.	1.852	0.647
Inability of the bank to monitor, analyze security incident and conduct forensic investigations due to lack of system event logs or due to audit logs that have been tampered with due to inadequate protection.	2.235	0.688
Malicious software installations that could lead to unauthorized access to or modification of information assets due to unauthorized users having permissions to install software on computers.	2.029	0.568

Proliferation of vulnerabilities that expose the systems to exploitation due to lack of adequate vulnerability management and patching of vulnerable systems.	2.088	0.612
Lack of necessary and adequate contractual clauses in contracts signed with third parties that indemnify the bank in the event certain agreements are breached by vendors.	2	0.485
Fines and penalties from regulators and contractors due to breach in contractual terms.	1.970	0.513
Inability of the bank to recover from a disaster due to untested disaster recovery and business continuity plans.	1.970	0.452

4.6 Relationship between Information Security Management Practices and Risk exposure

To find the relationship between the Information Security Management Practices and the Risk Exposures faced by the commercial banks in Kenya, a regression analysis was done. The results are indicated in the following tables.

Table 4.14: Regression Statistics

Regression Statistics	
Multiple R	0.902723574
R Square	0.814909852
Adjusted R Square	0.78185804
Standard Error	0.214187363
Observations	34

Table 4.15: ANOVA

ANOVA					
	df	***SS***	***MS***	***F***	***Significance F***
Regression	5	5.655512721	1.131102544	24.65552714	1.86627E-09
Residual	28	1.284534338	0.045876226		
Total	33	6.940047059			

Table 4.16: Coefficients

	Coefficients	***Standard Error***	***t Stat***	***P-value***	***Lower 95%***	***Upper 95%***	***Lower 95.0%***	***Upper 95.0%***
Intercept	5.203743274	0.304321799	17.09947592	2.36393E-16	4.580368328	5.827118221	4.580368328	5.827118221
FACTOR 1	-0.059270811	0.114200973	-0.519004429	0.607835873	-0.293200899	0.174659277	-0.293200899	0.174659277
FACTOR 2	-0.083156698	0.078860322	-1.054480831	0.300677401	-0.244694746	0.078381349	-0.244694746	0.078381349
FACTOR 3	-0.39834209	0.105185425	-3.787046462	0.000741546	-0.613804665	-0.182879515	-0.613804665	-0.182879515
FACTOR 4	-0.139351164	0.088440986	-1.57564009	0.126341508	-0.320514311	0.041811984	-0.320514311	0.041811984
FACTOR 5	-0.108994803	0.098283616	-1.108982431	0.276872421	-0.310319664	0.092330057	-0.310319664	0.092330057

4.7 Discussion

From the results on Table 4.14, the value of Multiple R shows a strong linear relationship between the variables with relationship strength of 0.90 on a scale of 0 to 1. In addition, 81.49 percent of the variables fall on the regression line based on the results indicated under R Square and with an adjusted R Square of 0.78 indicates that the independent variables are significant for this model. The standard error is also small at 0.21 showing that the points do not fall so far off the regression line.

Results from Table 4.15 also give the significance F as 1.86627E-09 which is less than 0.05 showing that our results are statistically significant and that the model used is ok.

Results from Table 4.16 show the individual p values for all the factors. From the factors in our model, factor 3 is the only factor that is statistically significant since its p value is less than 0.05. This means we can consider removing the other factors from our regression model. Factor 3 consisted of the variables: The bank has an information security policy in place that is regularly reviewed and updated in line with the technological trends in the industry. In addition, the bank maintains an up to date inventory of all its assets and their ownership is defined appropriately. Likewise, the bank has put in place appropriate system and application access control as per the access control policy e.g. password management and secure log on. The bank has also implemented physical entry controls to protect the premises, offices, data centers against unauthorized access and against environmental factors e.g. floods, earthquakes etc. In addition, the bank performs comprehensive backups for its systems regularly and that these backups are regularly tested to ensure the backups can be restored in the event of an incident.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter contains a summarization drawn from the data analysis, conclusions, contributions the study has made to theory and practice, recommendations for further research and limitations of the study.

5.2 Summary

This research work set out to achieve two objectives: To establish the extent of implementation of Information Security Management Practices among Commercial Banks in Kenya and the risk exposures. To this end, the questionnaires sent out included the management practices based on best practices and standards from which these practices are adopted. The extent of implementation across the banks has been summarized based on the means and standard deviations as summarized in table 10.

Another objective was to establish the relationship between the Information Security Management Practices and the risk exposures that banks face because of not implementing these practices. A regression analysis was done to determine this relationship and the equation on their relationship derived. From the regression equation, it indicates that there is an inverse relationship between the practices and the risks that the banks face.

5.3 Conclusion

Based on the objective of determining the extent of implementation of the Information Security Management Practices, we established that the banks have implemented the controls to a large extent. The controls that had been implemented to a moderate extent included proper segregation of duties, which could be attributed to organization sizes, inadequate implementation of cryptographic controls to secure data at rest and in transit, and the classification and labeling of data to avoid data loss. These two controls go hand in hand as proper classification and labeling will inform the cryptographic controls. However, the other controls were implemented to a great extent within the banks.

An analysis of the relationship between information security management practices and risk exposures reveals that implementation of these practices lowers the risk exposure. This has been determined by the regression equation that clearly shows an inverse relationship between the two variables. We can conclude therefore that the more the controls are implemented, the lower the risk the organizations face.

5.4 Recommendations

From the findings, it was observed that a few controls have been implemented to a moderate extent. These include classification and labeling of data, implementation of cryptographic controls, segregation of roles and duties, proper handling of storage media among other controls. We recommend that the banks put more emphasis in putting in place the necessary controls and pulling in the required resources to address these key risk areas.

5.5 Limitation of the Study

The research had limitations in that it highlighted the Information Security Management Practices and the information risk exposures on a high level without delving deeper to evaluate the underlying processes that contribute to the practices or the underlying exposures and practices contributing to the risks. As such, the preconceived risks and practices simplify the actual practices and risks in play.

The validity and reliability of the results is also a limitation. The respondents being the ones charged with overseeing the risk and security functions may not be willing to paint the true picture of the implemented practices and risks to which the bank is exposed. This is due to either self-confidence or fear that the research may be targeting their institutions and as such, they would not want to portray an inadequate or insufficient management of risk.

5.6 Suggestions for Further Study

This study only looked at the Information Security Management Practices in Commercial Banks in Kenya and the information security risk exposures these organizations face. Management practices as proposed by various standards and best practices were looked at together with risks arising from these practices not being implemented. A comparative study between various tiers of commercial banks can be done to determine the differences in the extent of implementation of these management practices and to determine the underlying reasons as to the differences if any. These differences can highlight key areas that management will need to prioritize to address the most prevalent risks in the organizations and the industry.

REFERENCES

Al-Ahmad, W., & Mohammad, B. (2013). Addressing Information Security Risks by Adopting Standards. *International Journal of Information Security Science, 2*.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study. *Computer & Security*, 432-445.

Aliyu, U. (2019). Significance of Information Technology in the Banking Industry. *International Journal of Informatics, Technology and Computers*, 15-19.

Antonucci, D. (2017). *The Cyber Risk Handbook - Creating and Measuring Effective Cybersecurity Capabilities.* New Jersey: John Wiley & Sons, Incorporated.

Australian Government. (2019, 4). *Australian Government.* Retrieved from Australian Government: https://www.cyber.gov.au/sites/default/files/2019-05/PROTECT%20-%20Essential%20Eight%20Explained%20%28April%202019%29.pdf

Bouveret, A. (2018, June). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.* Retrieved from International Monetary Fund: https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx

Central Bank of Kenya. (2017, May). *Central Bank of Kenya.* Retrieved from Central Bank of Kenya: https://www.centralbank.go.ke/wp-content/uploads/2017/05/Directory-of-Licenced-Commercial-Banks-Mortgage-Finance-Institutions-and-NOHCs.pdf

Central Bank of Kenya. (n.d.). *Bank Supervision*. Retrieved from Central Bank of Kenya: https://www.centralbank.go.ke/bank-supervision/

CISECURITY. (n.d.). *Cybersecurity-best-practices*. Retrieved from CISECURITY: https://www.cisecurity.org/cybersecurity-best-practices/

Communications Authority. (2019). *Communications Authority.* Retrieved from Communications Authority: https://ca.go.ke/wp-content/uploads/2019/03/Sector-Statistics-Report-Q2-2018-19.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Information Security*, 92-100.

Ela, M. (2011). A Framework for the Governance of Information Security in Banking System. *Information Assurance & Cybersecurity*, 12.

Ernst & Young. (2014, October). *EY's Global Information Security Survey 2014.* Retrieved from Ernst & Young:

https://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

First.org. (n.d.). *First.org*. Retrieved from First.org: https://www.first.org/cvss/

Gantz, S., & Philpott, D. (2012). *FISMA and the Risk Management Framework.* Massachusetts: Syngress.

Halibozek, E., & Kovacich, G. (2017). *he Manager's Handbook for Corporate Security - Establishing and Managing a Successful Assets Protection Program.* Oxford: Butterworth-Heinemann.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 243-248.

Horne, C. A., Ahmad, A., & Maynard, S. (2016). A theory on Information Security. *Australasian Conference on Information Systems.* Wollongong.

ICT Authority. (2016, June 20). *National ICT Policy.* Retrieved from ICT Authority: http:/icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf

International Organization for Standardization. (n.d.). *ISO/IEC 27001 Information security management*. Retrieved from International Organization for Standardization: https://www.iso.org/isoiec-27001-information-security.html

Javaid, M. I., & Iqbal, M. M. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). *2017 International Conference on Communication Technologies (ComTech).* Pakistan: IEEE.

Kabay, M. (1996). *The NCSA Guide to Enterprise Security.* NewYork: McGraw-Hill.

Knapp, K., Marshall, T., Rainer Jr, R. K., & Morrow, D. (2006). The Top Information Security Issues Facing Organizations: What Can Government do to Help? *EDPACS*, 1-10.

Kowalkowski, C., Kindstrom, D., & Gebauer, H. (2013). ICT as a catalyst for service business orientation. *Journal of Business & Industrial Marketing*, 506-513.

Ma, Q., Johnston, A., & Pearson, J. (2008). Information security management objectives and practices: a parsimonious framework. *Emerald*, 251-270.

Makumbi, L., Miriti, E., & Kahonge, A. (2012). An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector. *International Journal of Computer Applications*.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, 1-20.

NIST. (2014). *Cybersecurity Framework | NIST*. Retrieved from Cybersecurity Framework | NIST: view-source:https://www.nist.gov/cyberframework

PCI Security Standards Council. (n.d.). *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. Retrieved from PCI Security Standards Council: https://www.pcisecuritystandards.org/about_us/

Picot, A., Kranz, J., Gupta, M., & Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management*, 225-239.

SANS Website. (n.d.). *SANS Institute - CIS Critical Security Controls*. Retrieved from SANS Institute - CIS Critical Security Controls: https://www.sans.org/critical-security-controls/

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment. *Computer & Security*, 14-30.

Siponen, M., & Willison, R. (2009). Information security management standards: problems and solutions. *Information & Management*, 267-270.

T.Pereira, L.Barreto, & A.Amaral. (2017). Network and Information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, 1253-1260.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 4-19.

Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, 26-42.

Wright, M. (1999). Third generation risk management practices. *Computers & Security*, 9-12.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 583-592.

APPENDICES

Appendix I: Questionnaire

Dear Respondent,

This questionnaire aims at examining the Information security practices and the risk exposures among commercial banks in Kenya. The research is purely academic and any information obtained from this questionnaire will be treated with utmost confidentiality.

I will appreciate your and support and co-operation in your feedback.

Section A: Background Information

(Please tick and fill where appropriate)

1. What is the title/role of your position …………………………………………
2. How long have you worked in the department in that role………………….years
3. Please choose the below that apply to the qualifications you possess.
    - i. Diploma ( )
    - ii. Undergraduate ( )
    - iii. Postgraduate ( )
    - iv. Others specify ……………………

(Please tick and fill where appropriate for your organization information)

1. Which of the below best describes the ownership of your bank

    - i. Foreign owned ( )
    - ii. Commercial bank with government partly owning ( )
    - iii. Locally owned ( )
    - iv. Others specify ……………………..

2. How many employees does your bank currently have?
   ( ) 1 -200 ( ) 201 – 500 ( ) 501 – 1000 ( ) Over 1000

3. How many customers does your bank have?
   ( ) 1 – 10,000 ( ) 10,000 – 100,000 ( ) 100,000 – 1,000,000 ( ) Over 1,000,000

4. Does your bank operate in and outside Kenya?
   ( ) Yes ( ) No

5. Does your bank utilize cloud services (either as SAAS, PaaS, and IaaS)?

( ) Yes ( ) No

6. How long has the bank been in operation …………………. years.

Section B: Information Security Management Practices

For the below information security management practices, kindly indicate the extent to which each of them has been implemented in your bank.

Key: **1** – Not at all; **2** – To a little extent; **3** – To a moderate extent; **4** – To a great extent; **5** – To a very great extent.

#	**Information Security Best Practices**	**1**	**2**	**3**	**4**	**5**
1	The bank has an information security policy in place that is regularly reviewed and updated in line with the technological and business trends in the industry.					
2	The bank has designated roles and responsibilities for information security management and these have been allocated to individuals.					
3	The bank has properly done segregation of duties to avoid conflict of interest.					
4	The bank has ensured Information security has been integrated into all the projects carried out.					
5	The bank has instituted proper policies and controls for its mobile devices e.g. laptops, USB gadgets, tablet PCs etc.					
6	The bank has put in place mechanisms to ensure that employees and contractors are aware of the information security obligations.					
7	The bank maintains an up to date inventory of all its assets and their ownership is defined appropriately.					
8	The bank has properly classified and labelled its information assets and that proper security protection is accorded based on this classification.					
9	The bank properly manages information storage media and its movement or disposal is done in a way that the contents are not compromised.					
10	The bank has defined an adequate user access management for allocation, modification, removal/revocation of access rights and regular reviews of the access rights.					
11	The bank has put in place appropriate system and application access control as per the access control policy e.g. password management and secure log on.					
12	The bank has put in place cryptographic controls to secure data in transit as well as data at rest to protect it from eavesdropping and unauthorized access.					
13	The bank has implemented physical entry controls to					

	protect the premises, offices, data centers against unauthorized access and against environmental factors e.g. floods, earthquakes etc.					
14	The bank has put in place mechanisms to ensure ICT equipment and its supporting utilities e.g. electric power, air conditioning, cabling are properly secured and maintained.					
15	The bank has documented all its operating procedures and these are easily accessible, retrievable and applicable.					
16	The bank has instituted proper change management processes to all its ICT assets.					
17	The bank has put in place a system to monitor the capacity and performance of its networks, servers, facilities for proper management to avert incidents.					
18	The bank has implemented comprehensive technological solutions for its key security concerns e.g.an anti-malware solution, firewalls, Multi-Factor Authentication, email filtering solution, etc.					
19	The bank performs comprehensive backups for its systems regularly and that these backups are regularly tested to ensure the backups can be restored in the event of an incident.					
20	The bank has mechanisms and systems in place to ensure system user and administrator activities, exceptions are logged and that the logs are adequately protected from tampering and/or deletion.					
21	The bank has restricted permissions adequately to ensure only authorized personnel can install software on the servers and end user computers.					
22	The bank has a vulnerability management process to ensure that technical vulnerabilities are identified, patched and continuously monitored.					
23	The bank adequately manages its network security by employing network segmentation and limiting access to users and consultants to only those segments they need to access.					
24	The bank has ensured that policies and procedures are defined to protect the bank's information that is accessible to third parties in the supply chain and that these are agreed within the contracts and agreements.					
25	The bank has ensured that there are adequate Service Level Agreements defined in the contracts with third parties and these are monitored and reviewed to ensure they are met.					
26	The bank has a robust business continuity management process and that these are regularly tested and lessons learnt properly documented for improvement.					

27	The bank has identified and documented the set of legal, regulatory and contractual obligations to which it needs to be compliant with and that these are regularly reviewed for adequacy and completeness.					
28	The bank carries out independent reviews of the information security management and this is reported to management and that corrective actions are taken where appropriate.					

Section C: Information Security Risk Exposures

Kindly indicate the extent to which the bank is exposed to the risks in the table below.

Key: **1** – Not at all; **2** – To a little extent; **3** – To a moderate extent;
4 – To a great extent; **5** – To a very great extent.

#	**Information Security Risk Exposures**	**1**	**2**	**3**	**4**	**5**
1	Intentional or accidental exploitation of specific information security clauses/requirements that have not been defined in the existing information security policy.					
2	Ad-Hoc and improper information security management because there are no clear roles and responsibilities for information security defined and assigned to individuals.					
3	Inappropriate and unauthorized activities perpetrated by individuals intentionally or accidentally because of conflicting roles and areas of responsibility.					
4	Systems are commissioned with security vulnerabilities because information security requirements were not incorporated into the project life cycle.					
5	Reputational and legal risks arising from inadequate management of mobile devices.					
6	Breach of the requirements of the information security policy by staff and contractors due to lack of awareness creation and training making them unaware of their obligations to security.					
7	Loss of assets or introduction of malicious assets in the network arising from inadequate asset/inventory management.					
8	Legal and reputational risk arising from leakage of sensitive and confidential information to unauthorized people.					
9	Intentional or accidental manipulation of data due to excessive access rights provisioned to users coupled with lack of regular access rights reviews.					
10	Unauthorized and uncontrolled access to banks application systems due to inadequate access controls e.g. passwords,					

	2FA etc.					
11	Data loss/theft that is in transit or at rest due to improper application of encryption controls					
12	Unauthorized access to the banks premises, offices and data centers due to inadequate physical entry controls.					
13	Loss of assets due to inappropriate controls for removal of ICT equipment from the bank’s premises.					
14	Prolonged system outages because of lack of documented operating procedures that are easily accessible and easy to follow.					
15	System unavailability and unauthorized changes to bank systems because of absence of change management procedures or lack of adherence to them.					
16	System unavailability occasioned by lack of resource monitoring for capacity and performance.					
17	Hacking attacks on organization assets due to lack of implementation of appropriate and comprehensive technology controls e.g. anti-virus solution, firewalls, email gateways etc.					
18	Inability to recover from a security incident due to inability to restore backups since these backups are not frequently and adequately tested.					
19	Inability of the bank to monitor, analyze security incident and conduct forensic investigations due to lack of system event logs or due to audit logs that have been tampered with due to inadequate protection.					
20	Malicious software installations that could lead to unauthorized access to or modification of information assets due to unauthorized users having permissions to install software on computers.					
21	Proliferation of vulnerabilities that expose the systems to exploitation due to lack of adequate vulnerability management and patching of vulnerable systems.					
22	Lack of necessary and adequate contractual clauses in contracts signed with third parties that indemnify the bank in the event certain agreements are breached by vendors.					
23	Fines and penalties from regulators and contractors due to breach in contractual terms.					
24	Inability of the bank to recover from a disaster due to untested disaster recovery and business continuity plans.					

Appendix II: List of Commercial Banks in Kenya

1. ABC Bank (Kenya)
2. Bank of Africa
3. Bank of Baroda
4. Bank of India
5. Barclays Bank of Kenya
6. Chase Bank Kenya (In Receivership)
7. Citibank
8. Consolidated Bank of Kenya
9. Cooperative Bank of Kenya
10. Credit Bank
11. Development Bank of Kenya
12. Diamond Trust Bank
13. Dubai Islamic Bank
14. Eco bank Kenya
15. Equity Bank
16. Family Bank
17. First Community Bank
18. Guaranty Trust Bank Kenya
19. Guardian Bank
20. Gulf African Bank
21. Habib Bank AG Zurich
22. Housing Finance Company of Kenya
23. I&M Bank
24. Imperial Bank Kenya (In receivership)
25. Jamii Bora Bank
26. Kenya Commercial Bank
27. Mayfair Bank
28. Middle East Bank Kenya
29. National Bank of Kenya
30. NCBA Bank Kenya Plc.
31. Oriental Commercial Bank
32. Paramount Universal Bank
33. Prime Bank (Kenya)
34. SBM Bank Kenya Limited
35. Sidian Bank
36. Spire Bank
37. Stanbic Bank Kenya
38. Standard Chartered Kenya
39. Transnational Bank
40. United Bank for Africa[19]
41. Victoria Commercial Bank