EFFECT OF INFORMATION TECHNOLOGY RISK ON FINANCIAL PERFORMANCE OF COMMERCIAL BANKS IN KENYA

BY

WELDON SIGEY

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

DECEMBER, 2018

DECLARATION

I, Weldon Sigey, do make a declaration that this research project is my original work and has not been submitted for a degree award in any other university.

Signature……. Date……

WELDON SIGEY

D61/5826/2018

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

Signature……. Date……

DR. LUTHER OTIENO

ACCOUNTING AND FINANCE DEPARTMENT

SCHOOL OF BUSINESS

UNIVERSITY OF NAIROBI

ACKNOWLEDGEMENTS

I am very thankful to the almighty God for being in charge and granting me enough guidance, wisdom and courage as I wrote this research project.

I also have the privilege and honour to work with Dr. Luther Otieno and Dr. Nixon Omoro, committed and excellent mentors. Their tolerance, guidance and encouragement have been pivotal in completing this enormous task. I will not forget the effort put by Dr. Yabs, the coordinator, Eldoret Campus, in offering assistance necessary towards completing this project. It is my privilege having them as my teachers. I will extent my gratitude to the staff at the school of business, Eldoret Campus, for the constant push to ensure that I meet the stipulated timelines in as far as submitting my research paper is concerned.

To my fellow classmates, I am extremely grateful for the journey we have travelled together. Your support, ideas and criticisms have remained helpful in making my research project a success. I cannot dispense your contribution towards the success of this task. The respondents working in various commercial banks and business partners whom I was able to meet and seek clarification, I am thankful. Your openness and concrete information have driven me to this far.

To all, I am very grateful and God bless you abundantly.

DEDICATION

This research project is dedicated to my dear mother, Mrs. L. Bongon and my brother, Fr. Jonah Sigey, whose unwavering financial and emotional support, love and sacrifice throughout my academic work has rendered this piece of work a success.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CBK - Central Bank of Kenya

ICT - Information and Communications Technology

ISO - International Organization for Standardization

KBA - Kenya Bankers Association

NIST SP - National Institute of Standards and Technology Special Publication

ORM - Operational Risk Management

ROI - Return on Investment

3PL - Third-Party Logistics

ABSTRACT

The lending by commercial banks has a vital role in spurring the development of an economy. The existence of the commercial banks in any economy, thus, is inevitable since they affect almost all sectors of the economy. Consider the analogy that at the heart of every commercial bank is a technology company. The various activities relating to, financial services in banks are facilitated by technology and more importantly are the huge portions of capital investments and operational expenses that technology consumes. Commercial banks and how they perform financially depends on the reliability and security of its technology. A commercial bank and its customers can be sent into a frenzy when reports of a system downtime are announced. The changing technology landscape, especially the upsurge in information technology risk over the digital era, calls for banks to make strategic decisions on the technology to adopt. For example, weak controls allow a bank to be susceptible to processing errors or even unauthorized transactions. The study sought to establish the effect of information technology risk on Kenyan commercial banks performance in financial perspective. The study used descriptive statistic design and a population of 42 commercial banks registered and licensed by CBK were used as sources of data for analysis within a period of 5 years. The study focused on primary from the questionnaires as well as secondary data obtained from the banks' published financial statements from 2013 to 2017. The summary of the collected data was compiled by use of descriptive statistics that include the standard deviation and mean and were consequently analysed by use of the regression analysis and correlation techniques. From the findings, the study made the conclusion that strategic risk of IT, IT resiliency and continuity risk and technology vendor and third-party risk significantly and negatively affects performance of Kenyan commercial banks in financial perspective. The study further concluded that the banks are positively but insignificantly affected by cybersecurity and incidence response risk. The study recommends that Kenyan commercial banks should adopt IT risk management framework with policies that are aligned to their strategic objectives in order to mitigate the increasing IT risk in the banking industry.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The success of many businesses today is measured in terms of their ability to adopt and cope with modern information technology. Technology is considered as the most strategic capital investment to an organization. The rapid advancement of technology comes with information technology risk which like any other risk has a likelihood of altering the risk composition of the investment environment affecting the expected returns (Kozak, 2015). This study is focused on analysing the effect that information technology risk has on financial performance which measure monetary results of an organization's policies and operations. Information technology (IT) risk is generally any risk that is related to information. It is the risk to your business data, business process as well as the critical systems. ISO/IEC 2008 described the IT risk as the potential that vulnerabilities in an asset or a group of assets in an organization exist and that a given threat will likely and potentially exploit them. According to Stoneburner, Goguen, and Feringa (2002), an IT-related risk has a net mission effect which takes into consideration the probability that a particular information system vulnerability will occur as a result of a particular threat source taking effect and a resulting impact is likely to be felt.

Businesses today have most of their operations supported by information technology. The diffusion of information technology has been felt in many organizations and has targeted at minimizing costs by increasing efficiencies in service delivery. However, the risks that come with it has led to increase in cost of IT risk management. Information technology also facilitates interaction of financial institutions with vendors and third

parties subjecting the former to the assumptions in the transaction cost theory. Financial institutions will be affected by the two basic assumptions of bounded rationality and opportunism (Williamson, 1985). Suppliers can exaggerate their products and financial institutions on their side fail to scrutinize the products hence acquiring IT products and services that fall short of the required standards. Moreover, organizations including commercial banks are contingent upon such factors as environment, size and technology (Chenhall, 2007). The structure of organizations is under the control of internal as well as external factors and for efficiency and effectiveness, there should be suitability between the structure and the situational variables. However, technological environment where commercial banks operate is dynamic. Adapting technology which is compatible with the structure is a problem. Incompatibility result in IT gaps which expose a bank to IT risks.

Financial institutions are affected by information technology risk, commercial banks are not exceptional. The historical foundation of information technology in commercial banks is its use as a tool to support accuracy in financial services delivery. The fierce competition that characterizes the banking industry has prompted banks to widen the banking products and services they offer and consequently go digital where they offer their products and services off-site allowing their customers to access computers from their end. As a result of the widening scope of financial services, banks are facing greater threats attributed to the advancement in technological systems. More often do we hear cases of data theft attributable to cyber risk, bank accounts being compromised, destruction of various files, or the degradation of systems. Commercial banks face information technology risk due to the misalignment between the banks' business strategies and the IT strategies, the costly and complex IT environment as a result of the management decisions, and the mismatched and insufficient talent to deal with the

risk. The information technology in commercial banks with time becomes prone to obsolescence, disruption or lack of competitiveness hindering the agility of the information technology.

1.1.1 Information Technology Risk

Information technology (IT) risk refers to the existence of a given threat related to information technology with the potential of exploiting the vulnerabilities that exist in an organization's assets or group of assets (ISO/IEC, 2008). Data or information forms an important asset for every organization. According to Ryba (2005), IT risk is a threat that the application of information technology in an organization is not well implemented and does not operate as per the outlined assumptions in that such technology fails to meet the following key issues: fail to meet the organizational requirements and fail to ensure that appropriate integrity, security and availability are in place. Every organization has its own goals and objectives which can be long term or short term. As operations widen, it becomes necessary to put in place measures that encourages fast service to clients. Information technology serves the purpose well. However, it at times fails due to the threats involved.

The risk that is associated with the use and application of information technologies in organizations has been on the rise as the organizations' customers, business partners and outsourced operations increases. The progress in technology has led to dependencies within and without organizational framework (Rot, 2008). It has heightened the cases of diversities in operations, complexity of tasks, non-descriptiveness relating to various operations as well as quantity of risk factors. Organizations are facing dynamic development of information technologies which has significantly reduced the time that is required to appropriately and sufficiently react to the risk (Rot, 2008). The lack of the necessary preparedness in terms of reacting to

information technology risk may lead to collapse of an organization an implication that for a possibility of survival and development of an organization, appropriate reaction to IT risk is inevitable. As noted by Whitman and Mattord (2005), undoubtedly information communication technology has increased flexibility of time and place resources for the employees in an organization, but has also broaden the perception of increased information security risk from both internal and external attacks on information assets of an organization. This implies that the financial performance of organizations of organizations is at risk as information security risk increases.

1.1.2 Financial Performance

Financial performance is used to describe the degree at which the set objectives of an organization are achieved. It refers to the state at which the results of an organization's policies and operations are expressed in monetary terms (Verma, 2017). Warsame (2016) noted that through financial performance, firms show their ability to make good use of the resources they have at stake to ensure the attainment of the objectives and goals set. Financial performance entails the ability that a firm has to efficiently make use of the available resources, operate in a profitable manner, grow with time and coexist in the competitive environment (Kagoyire & Shukla, 2016).

Financial performance is measured by conducting the process of financial performance analysis. Verma (2017) noted that financial performance analysis takes into consideration analysing and interpreting financial statements in order to carry out a full diagnosis of the firm to ascertain its profitability and the general financial soundness of the business. The areas of financial performance analysis include the productivity performance, working capital performance, profitability performance, cash flow performance, liquidity performance, fixed assets performance as well as social performance (Meigs, 1978; Metcalf & Titard; 1976). Through the different ratios (ROI,

ROE, efficiency ratios, profit margin, liquidity ratios, among others), the financial performance of a firm can be established. The overall performance of a firm is measured by use of ROA which is a ratio of the income earned by a firm to the total assets owned by the firm.

Financial performance of an organization is a pertinent issue which captures the attention of a number of stakeholders affected by the results of a financial performance analysis. The interested groups include trade creditors, bondholders, investors, employees, suppliers and the management. They can either be affected directly or indirectly by how a firm makes use of its resources (Meigs, 1978). The future of every firm can, therefore, be ascertained to a bigger extent by considering its financial performance which tells more on the financial soundness and health of the firm (Ehrhardt & Brigham, 2008).

1.1.3 Information Technology Risk and Financial Performance

Managing the risk-return trade-off is imperative for commercial banks as a way to attaining an optimal profitability. The application of information technology has become a major way for commercial banks to gain competitive advantage. According to the study carried out by Wang, Lai and Zhao (2008) on the "impact of information technology on 3PL firms in China," IT significantly improves 3PL firms' financial performance. The study resolved that 3PL firms should strategically adopt IT in their operations and commit their resources in order to better their financial performance. The daily emergence of new information technologies is accompanied by a surge in information technology risk among commercial banks. Information technology risk, therefore, becomes among and part of the core risks that inhibit the income generation activity of commercial banks.

There has been an upsurge in debates with regard to the IT risk in the recent past. The threat posed by information technological risk in the banking sector is mightier and affects the solvency of most of the banking institutions. Most banks, both locally and internationally, have gone to losses has a result of hackers and attackers who encroach their systems to steal valuable banking information. The reliance of computer hardware, software, telecommunication systems, electronic devices as well as online networks by commercial has witnessed their vital data being damaged, loss of the data, their rights to own assets being violated, system failures, disruptions of their operations, defects in software and operating mistakes, all originating from technology risks. According to the Management Authority of Singapore (2008), information is a basic internet service which characterize internet banking.

It is through the information that all online transactions and communications are accomplished. The interaction of stakeholders of a bank (customers, suppliers, other financial institutions, government) with the bank becomes complete with the presence of information service. However, the internet banking containing the information service are often the targets for malicious parties including hackers who aimed at vandalizing and mutilating the original information that a bank was providing (Monetary Authority of Singapore, 2008).

The issue of information technology risk and financial performance, and consequently the effect the former plays in the latter has become a focal point of discussion among all financial institutions. The Government of Kenya (GoK) in 2013, through CBK, issued risk management guidelines including ICT risk management policy; information security; encryption technologies; ICT internal and external audit, among many other

concerns an indication of the weight that GoK attaches to information technology risk and the fact that it can adversely affect the banks performance in financial perspective. The concerns are aimed at preventing all manner of bank frauds. It is worth noting that CBK regulates the banking industry in Kenya and works to ensure that they remain financially stable at all times.

1.1.4 Commercial Banks in Kenya

The CBK annual report for the year ended 2017 had it that the banking sector in Kenya is composed of 42 commercial banks, 1 mortgage Finance Corporation and 13 deposit taking microfinance institutions. Moreover, the sector has 3 credit reference bureaus, 8 representative offices and 115 foreign exchange bureaus (CBK, 2018). According to the Annual Supervisory Report of 2012 by CBK, there were 43 banks but as a result of Charter House Bank being defunct, the number of commercial banks remained at 42. Out of the 42 commercial banks, two are under receivership, namely; Chase Bank Kenya and Imperial Bank Kenya (Kenya - Chase Bank under Receivership, 2016; Press Release, 2015). These commercial banks have their headquarters based in the Capital City of Kenya, Nairobi. According to Ayugi (2016), CBK uses the tier system of classification where commercial banks have been classified in three tiers; tier 1 comprising of large banks, tier 2 made up medium-sized lenders and Tier 3 composed of small-scale lenders, holding 49.9%, 41.7% and 8.4% market shares respectively.

The banking industry in Kenya, both commercial and privately owned, operates under the regulations provided by four authorities: The Companies Act, The Banking Act, The Central Bank of Kenya Act and The Prudential Guidelines issued by the CBK. The CBK falls under the Ministry of Finance and is tasked with the formulation of the monetary policies that aim at attaining the stability of prices as well as issuing of currency. The CBK Act provides that CBK has a role to promote the financial stability

by regulating, supervising and licensing financial institutions (CBK, 2017). Generally, the CBK works towards ensuring that the financial system is liquid, solvent and functioning properly. The monetary policies that CBK comes up with are essential in keeping check of the economy in general and ensuring that it operates in a fair way which does not harm the financial system. The banks in Kenya have also strive to come as one and form the Kenya Bankers Association (KBA), an association which advocates for the rights, interests as well as ensuring that other issues affecting the member institutions are resolved.

The commercial banks are vital in the economy and play a number of roles including providing safe keeping of clients' finances, facilitating the transfer of money from an account of one person to an account of another person, offering lending services to their customers in form of loans, offering foreign exchange services to their customers where they sell foreign currencies at market value to their customers, facilitating international trade by issuing bank statements to their customers who deal in imports and exports to prove their credit worthiness, offering investment services to their clients where they can act as intermediaries in selling shares of companies to their customers and even selling their own shares to their customers, giving financial advice to their customers on the business practices that they can engage in to maximize their returns, safe keeping of customers' valuables like title deeds and expensive jewellery, offering advice on taxation matters to their clients including the filing of tax returns and finally commercial banks in Kenya acts as trustees where they are responsible in managing the property upon death of the owner on behalf of the family or those to take over the property of the deceased.

The Kenyan banking industry has witnessed significant growth over the past few years. This has spurred the country's economy by a bigger margin. The growth in commercial banks has motivated the adoption of information technology in order to serve their clients faster, efficiently and effectively. Most importantly for commercial banks is the fact that information technology has become a criteria for measuring a bank's competitiveness over others. However, the information technology has attracted risks associated with insiders and outsiders who want to unfairly benefit from the vulnerabilities that exist in the application of technologies. Information technology risk take into account among others, the failure of commercial banks to meet the technology requirements leading to inconvenience among their clients, lack of integrity in the development and implementation of systems, availability of security threats, bank accounts being compromised, destruction of bank's files, degradation of a bank's system and data theft.

1.2 Research Problem

A fundamental assumption of recent research done on the subject of information technology risk indicate that information technology (IT) risk has a direct bearing on financial performance (Economist Intelligence Unit, 2012). The financial performance of commercial banks is dependent upon several factors, one of them being information technology. Information technology has contributed to various innovations among organizations and boost their productivity and financial performance (Romdhane, 2013). The current environment in which banks operate is marred with constant advancement in technology. This has attracted the attention of regulatory authorities in the banking industry. They have consequently put in place measures and constantly warns the stakeholders in the industry of the dynamic technological environment that they operate in and the risks that come with it. Though some of the past studies view

information technology as having positively contributed to financial performance and hence the benefits supersede the challenges brought about by IT risk (Wang, Lai & Zhao, 2008), there is a need to address the significance of IT risks on banks performance in financial perspective.

The world is losing millions of dollars attributed to IT risk. In Kenya, adoption of technology is rapidly increasing. Financial institutions in Kenya are increasingly adopting new information technologies. Therefore, IT risk is on the rise. Though not much is reported by financial institutions on cases of technological frauds, financial institutions are losing millions of Kenyan shillings. It is commonly known that the IT risk cuts across all industries in the economy but the study by Economist Intelligence Unit (2012) stresses that the banking industry have especially broad concerns in relation to IT risk and aspects of reputational risk. Commercial banks in Kenya are the providers of the critical daily and increasingly online services to their clients, heightening IT vulnerability in the banking industry. This virtually puts the information technology of commercial banks at risk. The role they play as custodians of assets for their clients makes banks delicate in as far as IT failures are concerned since it makes it possible for miscreants carry out money theft directly or by capturing the confidential data belonging to customers.

Technology has been growing over the years and is the greatest innovation that is changing the way we do business. Information technology has been perceived as a basis for competition among organizations. Some studies in the past have portray information technology as contributing to performance by organizations (Romdhane, 2013; Wang, Lai & Zhao, 2008). However, Kamau (2010) recognized credit, operation, reputation and compliance risks as critical risks negatively affecting performance of organizations. It is good to note that operation, reputation and compliance risks are IT risks. This was

supported by Rot (2008) who argue that the failure by IT management processes in organizations to carry out risk assessment raises costs. To bring a consensus on these varying perceptions on IT and the risk involved is to find out the effect of information technology risk on financial performance of commercial banks.

The overall objective of this study was to investigate the effect of information technology risk in the financial performance of Kenya's commercial banks in the banking industry and generally make a contribution to the existing literature in as far as the subject matter is concerned. Thus, the research question, "Does information technology risk affect the financial performance of commercial banks in Kenya?"

1.3 Research Objective

To determine the effect of information technology risk on financial performance of commercial banks in Kenya.

1.4 Value of the Study

Many parties will gain from this study. The first group involve commercial banks themselves, specifically the board of management, CIO, CRO, CTO as well as risk and compliance personnel, who will get a blueprint on the effect that information technology risk have in financial performance of commercial banks and consequently use the findings as a guideline to adopting good IT risk management policies which will safeguard the interests of all stakeholders in the organization. The study will be insightful to the executives on being aware of the specific IT risks and how they can handle them in order to enhance the profitability of commercial banks and their general optimal financial performance while at the same time ensure that commercial banks are conforming to the set rules and regulations under the CBK Act, the Companies Act and the Banking Act.

Policymakers will also be among the big beneficiaries to use this study. They include the government and the CBK who are involved in formulating and implementing monetary and IT regulatory policies. The policymakers like the CBK will be in a position to know the impact of the policies that they have put in place in as far as IT is concerned. Therefore, they will be in a position to amend the existing policies to suit the current technological trends and ensure the rights of all stakeholders are being protected. The government will derive knowledge from this study which aids in issuing guidelines to commercial banks on the effective IT practices.

The academic world, researchers and academicians, will have a pool of knowledge from the research findings from this study. The study, therefore, will add to the existing literature on the effect that information technology has in commercial banks financial performance in Kenya. It also lay out a foundation for the researchers who would like to research on the same subject whereby they can identify the knowledge gaps and carry out further studies relating to this area of study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Chapter two is focused on the literature already existing regarding the effect of information technology risk on banks performance in financial perspective. The literature review further discusses the various theories and models which forms the foundation of this research work. The chapter also present the specific IT risks and their effect on the bank's performance in financial perspective; the empirical review of the literature previously done by various authors related to the subject matter; a summary of the empirical review and finally highlight the conceptual framework where the entire research will revolve around.

2.2 Theoretical Review

2.2.1 Introduction

The theoretical section provides highlights on the previously established theories including diffusion of innovation theory, transaction cost theory and contingency theory approach; which underpinned this particular study. The first theory is concerned with how new technologies spread in the society, get adopted forming part of the culture of the society but, however, comes with complexities and risks which increase the cost of risk management. The other two theories are concerned with the increased costs to organizations associated with information technology risk.

2.2.2 Diffusion of Innovation Theory

The theory is the work of Rogers who developed it in 1962. Diffusion of innovation theory explains the generation of a new idea, how it gains momentum over time and eventually spreads through a social system. The aftermath of the diffusion is people to

adopt the new idea and shift from their previous way of doing things to new one. Interaction of many factors including communicating the idea, time taken by the idea to diffuse through the population and the society in which the idea is being introduced (Rogers, 1995). The diffusion in idea end up inculcating a culture in people who adopt the idea over time. The diffusion of innovation theory has been in used extensively in technology and economics for quite some time now. The diffusion theory has played a great role in information technology in development of other theories like developer-based theory and adopter-based theory which are key in explaining the diffusion of various innovations in the society (Surry, 1997).

Diffusion in information technology is, however, characterized by risks associated with technology and internet penetration. Technological risk occurs in many forms which include simple malfunctioning of computer, phis as well as complex malicious acts by attackers like cybercrime. The risk has heightened costs associated with risk management process whereby financial institutions including commercial banks have to incur have to incur huge amount of funds to implement strong IT risk management techniques. It is only those commercial banks which are considered large in terms of the capital base and market share that are capable of implementing the strong IT risk management techniques.

2.2.3 Transaction Cost Theory

Transaction cost theory is founded on two basic assumptions (Williamson, 1985). First, the theory is founded on bounded rationality. This assumption asserts that there is a cognitive limitation of the human mind which often rules out the complete process of evaluating the possible consequences resulting from decisions made. In the context of IT risks among commercial banks, this assumption relates closely with the technology vendor and third-party risk. Commercial banks do outsource IT services and, in most

cases,, they are subject to bounded rationality where they lack sufficient knowledge and skills to specify IT requirements, select appropriate IT suppliers as well as manage and control the relationship. The second assumption is that of opportunism whereby IT suppliers can take advantage of the insufficient IT knowledge and skills among commercial banks to lie or sell them IT services which are exaggerated but does not meet standards exposing their clients to IT risks.

The assumptions of bounded rationality and opportunism as a result of outsourced applications by commercial banks give rise to certain transaction costs which the organizations have to incur including the costs of carrying out searches, the costs of selection, the costs of engaging in bargaining, the costs of enforcing agreed upon terms and conditions and costs of coordinating work. Commercial banks have to incur these costs in order to acquire IT services that meet their requirements. The newer information technologies emerge, the higher the cost of transactions due to the complexities and risks which come with it.

2.2.4 The Contingency Theory Approach

Corporate theories researchers believe in an optimized organizational structure and that there is a possibility of determining such organizational structure (Weber, 1946; Fayol, 1949). However, the reality may be different due to considerable changes surrounding organizations. Modern researchers have argued that the attestations by previous researchers like Weber, Taylor and Fayol are failed one's sine corporate governance as well as organizational structures are affected by random factors. The effectiveness and better performance of a corporate are dependent on the suitability to structure as well as organizational contexts like environment, size and technology (Chenhall, 2007). Contingency theory is a form of a suitability theory which explains suitability between organizational structure and situational variables. Organizations do face a lot of

pressure from both internal and external factors. Organizing the structure of an organization will, therefore, depend on the organizational environment of the activities of the organization (Scott, 1992). The situation will have to be in tandem with an organization structure so as to foster good performance in an organization.

The technological situation under which commercial banks operate is that which is dynamic and is characterized by day-to-day changes. These changes are followed by increase in incompatibilities between the changing IT environment and the structure of commercial banks resulting in gaps. In case of the incompatibilities, commercial banks have to incur costs of acquiring new information technologies with compatibility capabilities with the operating environment and that address the current customer needs. Moreover, the IT gaps created by changing technological environment allow attackers to access and steal information assets of a commercial bank which consequently result in losses.

2.3 Specific IT Risks in the Banking Industry

This part deal with the specific IT risks that affects the performance of the Kenya's commercial banks.

2.3.1 Strategic Risk of IT and Financial Performance

In a dynamic world, ineffective IT strategy becomes among the top threats that a financial institution faces. A financial institution faces an uphill task in trying to balance the risk of whether to adopt a new technology or simply ignoring it and watching events as they settle (Deloitte, 2018). Financial institutions also face disintegration between IT and business strategies. As a result of that, inappropriate investments and misaligned expectations are experienced. The IT strategy adopted should be able to support evolving business priorities and operating models as well as provide an enabling

environment for agile responses to developments in the market. Moreover, there is a departure by financial institutions from outmoded technologies like data centres, platforms as well as applications to new ones. Banks can, however, retain some of the old technologies to serve specific interests like supporting select geographies, custom products or even unique products but this will increase complexities within the bank and also raises costs to maintain them. When such happens over several applications, a financial institution will find itself hamstrung by its own technology (Svata & Fleischmann, 2011).

As posited by Andries et al. (2018), there is a need for an institution to define its IT strategy or align its IT strategy with the business needs in order for the organization to succeed in meeting its institution's requirements. Misalignment, however, will compromise the achievement of an organization's commercial and financial objectives. Barret (2016) added that the relation that exist between unmanaged IT risk and the performance of financial institutions in financial perspective including is inverse.

2.3.2 Cyber Security and Incidence Response Risk and Financial Performance

Cyber security has become a key concern in the agendas of many boards in most of the major companies as a result of the several incidences of cyber-attacks, breaches in data privacy and misconduct. It is important to point out that the exercise of vigilance in cyber security through access controls, and security protocols should not hinder the efficiency of doing business by organizations (Svata & Fleischmann, 2011). The failure in cyber security arouses a cyber incident response (CIR) (Deloitte, 2018). An organization should then be aware of the probability of a cyber incident so that it can launch a solid and well-tested CIR plan. The responses should be proportionate to the incidents that have occurred and should cover such aspects as technical, communication, and compliance as well as forensic. Upon a cyber security failure, CIR

should prioritize to secure digital evidence, to restore operations, and to notify the senior management and affected stakeholders as well as regulatory authorities (Pfeiffer, 2015). All these are aimed at minimizing further losses and stabilizing the financial position of the involved institution.

According to the Kenya Cybersecurity Report of 2016 by Serianu Ltd. in partnership with United States International University-Africa, the financial sector is the most affected sector by cybercrime. The report further indicated that there has been a growth in the cybercriminal activity in Kenya targeting both public and private organizations (Kaimba et al, 2016). The activity is pursued by an insider or outsider including attackers and terrorists which when they successfully execute their heinous acts result in an organization losing revenue, sensitive information, consumer and constituent confidence eroded as well as denial of business operations. Notably, the cost of cybercrime in Kenya has rose to a whopping $175 million in 2016 from $150 million in 2015 (Kaimba et al, 2016). The high cost is attributed to lack of adequate response mechanisms, and lack of security awareness, among other concerns.

2.3.3 IT Resiliency and Continuity Risk and Financial Performance

Financial institutions are virtually operated using technology with all their services provided by application IT. The IT should, therefore, be resilient in times of disruptions and outages. According to Rai and Mohan (2006), the technological environment has been changing and commercial banks have to have the capability of developing customized range of products as well as convenience at low cost to meet customers' changing needs. They noted that organizations should be characterized by resiliency standards which enables its resiliency capabilities to allow technology which supports the most critical businesses in the organization. An end-to-end view of technology is necessary to support the critical processes such that an organization is certain of

recovery upon disruptions. Recovery testing should be rigorous with ability of the recovery plans to work (Maina, 2012). However, most institutions may do a one-off testing of a technology application used instead of conducting a comprehensive test on a technology that supports end-to-end processes like settlement or clearing (Deloitte, 2018). Also, there are quite a number of financial institutions which outsource critical technology services from third-party providers of which the institutions have to understand the third-party resiliency as well as recovery capabilities to an extent that the technology seems to be owned by the institution.

2.3.4 Technology Vendor and Third-Party Risk and Financial Performance

As a financial institution enter into agreements with vendors and service providers, partners and other third parties who are proliferate in financial services, institutions do assume new risks as well. Basel Committee on Banking Supervision (2005) noted that technology risk originating from a third party is capable of generating reputational, financial, operational and other risks which affects the financial performance of an institution. It calls for a financial institution to be cognisant of the standard forms of assurance that vendors provide as well as ascertain their due diligence. KPMG in their report of 2014 on 'Third-party risk management' asserted that due diligence, contracting and monitoring procedures ought to be developed and implemented by a financial institution on the third parties they deal with. (KPMG, 2014). The technology vendors engaged by the IT department of a financial institution have to go through the same procedures. Areas of concern when carrying out due diligence on third parties and that can adversely affect financial performance of an institution include financial viability, third-party reputation, compliance, and strategic alignment, among other attributes (Deloitte, 2018).

According to Murambi (2016) Kenya's commercial banks and their IT departments ought to take the lead in assessing the third parties IT capabilities irrespective of whether the third-party offers support to the institution relating to IT or business or both. An overall understanding of a third-party's technology management processes is pivotal to ensuring mature capabilities of the financial institution in assessing third-party cyber and business continuity risks. For example, ineffective technology change management processes of a third party have a tendency to increasing the risk of disruption of service provision.

2.4 Empirical Review

Harle, Havas, Kremer, Rona and Samandari (2011) in their article "The future of bank risk management" discussed the issue of IT and IT risks in future and how banks will manage them. According to the authors, the emergence of new technology brought about change in customer behaviour as well as enabling new techniques that enhance management of risks. They argued that upon the proliferation of new technologies, banks have experienced computing power which is relatively cheap and fast as well as convenience in storing data which has enabled risk decision support while at the same time integrating processes. Banks can easily access data regarding their customers in order to make good decisions on credit issues. However, Harle and his colleagues opine that in the next ten years many unknown innovations are likely to be realized which will either expose banks to the positive implications or affect them negatively. Easy and faster access to customer data can be an opportunity for scrupulous people to take advantage and steal or alter confidential customer information. The authors further explained that the emergence of new technology has led to increased dependence on models by bank managers which despite the increased availability of data and advanced

computing, modelling and algorithm, has led to poor decisions being made and increase in bank's IT related risks and consequently losses.

The study by Rot (2008) on IT Risk Assessment using the Quantitative and Qualitative Approaches focused on examining the impact of the IT risk assessment techniques in the risk management process. In the study, Rot noted that the advancement in technology and the correlation between organizations and customers, partners and third parties has brought about complexities and risk factors to the business environment. IT assessments, therefore, become crucial in order to strike a balance between threats affecting IT and the costs incurred in protecting IT systems. However, the author asserted that the lack of preparedness in terms of carrying out risk assessment well in advance and using a combination of the appropriate quantitative and qualitative techniques can lead to collapse of an organization. The aim of an IT risk management process is to correctly undertake the minimization of losses associated with the risk. Furthermore, Rot described an IT risk as that threat to an IT system in an organization which results in either or all of the following: failure of IT to fulfil or rather meet business requirements; inability of the IT to ensure appropriate integrity, security as well as availability; and inappropriate implementation of an IT, thus failing to work in accordance with the laid down assumptions. Therefore, IT risk is deemed to increase cost.

The study done by Kamau (2010) on adoption of risk management by Kenyan banks was based on 44 commercial banks actively operating Kenyan banking industry based on data from CBK 2010. This study was focused on identifying the risks that commercial banks face as well as the strategies that they put in place to mitigate the risks. A census involved all the licensed Kenyan commercial banks and risk management staff were administered with questionnaires. Analysis of data was done

using SPSS and results graphically presented and tabulated. Study recognized credit risks, operational risks, reputational damage and compliance risks as the most critical ones affecting the performance of commercial banks. It is good to note that reputational and technological compliance risks are IT risks.

Jowi and Abade (2016) covered a study on evaluation of information security risk assessment for internet banking among commercial banks in Kenya where they employed a descriptive research design, a census of 43 commercial banks, administration of questionnaires departmental staff managers, use of SPSS for data analysis and present data using frequency distribution tables and percentages. The study found out that most commercial banks are aware and use the risk management framework. Other variables that Jowi and Abade established include a situation where policies and procedures fail, poor training of employees, inadequate internal audit and unguaranteed supervision of staff, all the factors relate to IT either directly or indirectly and affects the financial performance of commercial banks.

2.5 Summary of Empirical Review

From the review of the previous studies, it becomes clear that information technology risk affects performance of Kenyan commercial banks in as far as financial perspective is concerned. However, most of the studies carried out as revealed under the review focus on general risk management and technological innovations and their effects in financial performance of commercial banks. Therefore, a few research studies have been focused on IT risk and its effect on financial institutions.

Considering IT risk in the banking sector, it becomes elusive that the effect of IT risk on performance of commercial banks in financial perspective is still a green area demanding for extensive research. This become a driving force towards accomplishing

this study and establishing the effect that IT risk have in Kenyan commercial banks in in as far as their performance financially is concerned.

2.6 Conceptual Framework

The study is focused in establishing the effect of IT risk on financial performance of commercial banks in Kenya. Independent variables for the study was strategic risk of IT, cybersecurity and incidence response risk, IT resiliency and continuity risk and technology vendor and third-party risk while the dependent variable was financial performance.

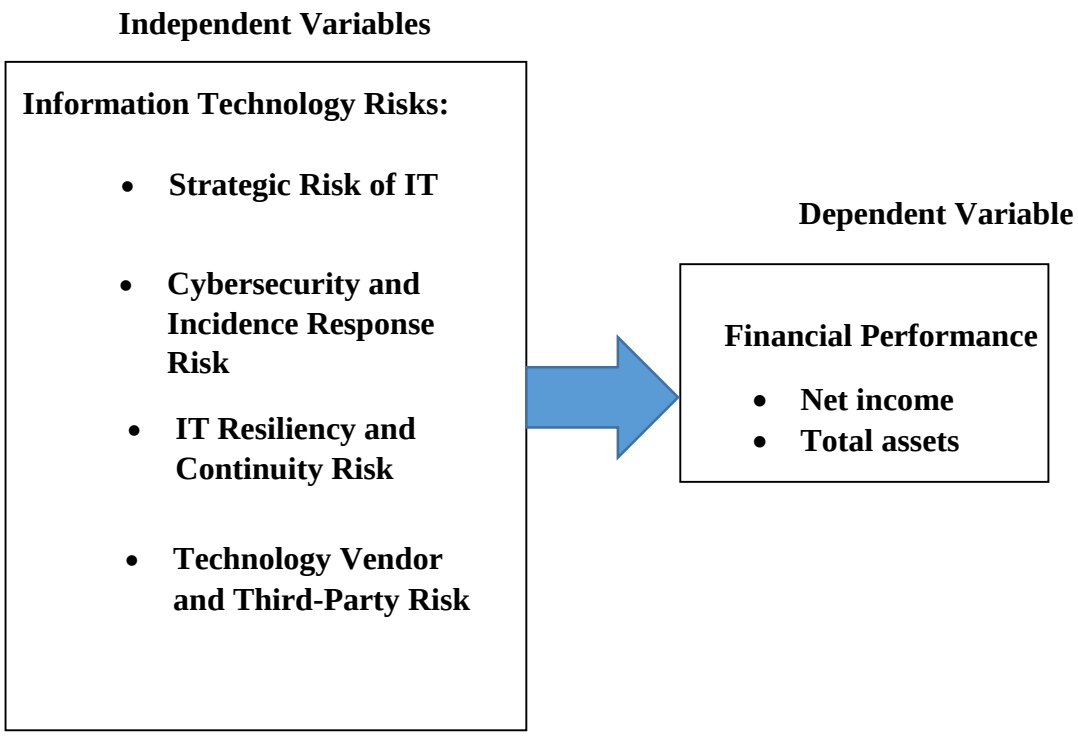

Figure 2.1: Conceptual Model

Source: Author (2018)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Chapter three focuses on the research design, the study population, data collection techniques and the data analysis techniques.

3.2 Research Design

Research design refers to an overall strategy that a researcher adopts to help to integrate different components of a study in a manner that is coherent and logical and, thus, ensure that the study's research problem is addressed in an effective way (De Vaus, 2001). Research design constitutes a blueprint that aids in the collection, measurement as well as the analysis of data. A descriptive research design was adopted in this study where the characteristics for the variables that was used in the study are explained. The research design was appropriate for the study as it explained the effect that information technology risk has on financial performance of commercial banks in Kenya.

3.3 Study Population

A population as a set of all subjects (items or people) that a researcher is set to study and make statistical inferences relating to the same (Yount, 2006). The population that was used to carry out this study is comprised of all the 42 Kenya's registered commercial banks (CBK, 2017). The researcher conducted a census survey due to the small number of commercial banks in Kenya.

3.4 Data Collection

Questionnaires were the instruments used in collecting primary data for this study. The items in the questionnaires relate to the IT risk which specifically address issues on strategic risk of IT, cybersecurity and incidence response risk, IT resiliency and

continuity risk and technology vendor and third-party risk. The questionnaires also comprise of structured questions presented in form of a Likert Scale rated 1-5. The questionnaires were administered to the IT officers, business partners and other relevant parties of the 42 commercial banks in Kenya. Secondary data were obtainable from the published financial statements of the banks for a period of 5 years.

3.5 Data Analysis

The collected data was examined and checked to ensure that they are complete and comprehensive. The questionnaire was edited to ensure that it was comprehensive and could not confuse the respondents. Tables was used for data presentation for easy understanding, interpretation as well as analysis. The collected data was finally summarized with the aid of descriptive statistics techniques like standard deviation and mean. Correlation and regression analysis will be the appropriate tools to analyse the data.

3.5.1 Analytical Model

The regression equation was generated as follows

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

Where: Y stands for ROA. ROA= Return on assets, a ratio indicating net income to total assets; α is a Constant term; $\beta 1$, $\beta 2$, $\beta 3$, $\beta 4$ represents Coefficients to the regression model; $X1$ stands for Strategic risk of IT; $X2$ stands for Cybersecurity and incidence response risk; $X3$ stands for IT resiliency and continuity risk; $X4$ stands for Technology vendor and third-party risk; and μ stands for Probable error which captures the variables that are not included in the model.

Operationalization of Variables

Variables	Notation	Measurement	Source
Y	Financial performance	Net Income/Total assets (ROA)	Financial book statements
$X1$	Strategic risk of IT	Likert scale	Questionnaire
$X2$	Cybersecurity and incidence response risk	Likert scale	Questionnaire
$X3$	IT resiliency and continuity risk	Likert scale	Questionnaire
$X4$	Technology vendor and third-party risk	Likert scale	Questionnaire

3.5.2 Test of Significance

The P values was used to establish the significance of variables at 5% level of significance where a P-value greater than 5% was considered insignificant ($0.05<P$) while a P- value less than 5% ($P<0.05$) was considered significant.

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND INTEPREETATION

4.1 Introduction

Chapter four is an outlay of results involving analysed data which are tabulated. The chapter gives a description of the response rate, the reliability of data as well as descriptive statistics, results of correlation analysis, results of regression analysis and the interrelation of study findings.

4.2 Response Rate

The research used a census survey whereby the 42 commercial banks in Kenya were issued with questionnaires. Complete data was, however, obtainable from 39 commercial banks representing a response rate of 92.86 percent which was appropriate for the study. The high response rate achieved in the study was a result of the researcher's efforts in collecting data, administering questionnaires and making follow-ups.

4.3 Data Reliability

The reliability of the research instrument used in the study was determined using Cronbach alpha, a statistical tool that provides measurement to ascertain internal consistency of a research instrument. Table 4.1 shows the results obtained

Table 4.1: Data Reliability

Variable	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Strategic risk of IT	.902	.902	4
Cybersecurity and incidence response risk	.894	.894	4
IT resiliency and continuity risk	.858	.865	4
Technology vendor and third-party risk	.748	.750	4

Source: Research Findings (2018)

The Table 4.1 above shows that strategic risk of IT, cybersecurity and incidence response risk, IT resiliency and continuity risk and technology vendor and third-party risk yielded alpha coefficients of 0.902, 0.894, 0.858 and 0.748 respectively. The alpha values are above 0.7, an indication that the questionnaire used for this study was reliable. As Bryman & Bell (2007) posited, the Cronbach alpha coefficient of 0.7 and above is a clear indication of reliability in as far as the instrument used to collect data is concerned.

4.4 Descriptive Statistics

Table 4.2 is a presentation of the descriptive statistics of the study comprising of the mean, the standard deviation as well as kurtosis.

Table 4.2: Descriptive Statistics on Information Technology Risks

	ROA (Ratio)	Strategic Risk of IT	Cybersecurity and Incidence Response Risk	IT Resiliency and Continuity Risk	Technology Vendor and Third-party Risk
Mean	.01907	3.23080	3.84620	3.82690	3.79490
Std. Deviation	.03262	1.22257	.91518	.98032	.99979
Kurtosis	4.188	-1.357	.493	-1.456	-.878

Source: Research Findings (2018)

The study revealed that the average performance of Kenya's commercial banks in financial perspective as indicated by ROA is 0.01907, a standard deviation of 0.03262 and a relatively peaked distribution as shown by the KURT of 4.188. The implication here is that the existence of information technology risks lowers the financial performance of commercial banks. The table 4.2 indicated that commercial banks experience strategic risk of IT to a moderate extent as indicted by a mean of 3.23080 with a standard deviation of 1.22257 and a relatively flatter distribution as indicated by a negative KURT of -1.357. This demonstrated that commercial banks are faced by various strategic IT risks including the ineffective IT strategy whereby the IT strategies and business strategies are disintegrated. The banks, therefore, become victims of inappropriate investments and misaligned expectations. With old technologies retained, commercial banks are met with high costs.

The findings relating to rating of cybersecurity and incidence response risk and its effect on financial performance had a mean of 3.84620, standard deviation of 0.91518 with a relatively flattened distribution as indicated by the positive KURT of 0.493. The findings demonstrated that commercial banks are affected to a great extent by cybersecurity and incidence response risk. Commercial banks experience incidences of cyber-attacks at a high rate. They are also faced with breaches in data privacy and misconduct. The study also found out that banks do not have effective and efficient cyber incident response (CIR) plan often leading to disruptions of cash flows when cyber-attacks and other data breaches occur which lower their financial performance.

The mean on the effect of IT resiliency and continuity risk was 3.82690, standard deviation of 0.98032 and a negative KURT of -1.456 indicating a flatter distribution. This indicated that performance of commercial banks in financial perspective is affected by IT resiliency and continuity risk to a great extent. They are characterized

by ineffective and inefficient recovery testing which is attributed to lack of regular update of the security controls and IT tracking processes to cope with the changing technological environment. The study further found out that banks lacks adequate resiliency capabilities in times of IT disruption and outages which causes losses due to halted operations and high costs of recovery of the lost data. Banks also do not fully adhere to their standards and policies on business partners and other third-parties, hence, the inadequate third-party resiliency and recovery capabilities.

From the table, the mean on extent of effect of technology vendor and third-party risk was 3.79490, standard deviation of 0.99979 and a negative KURT of -0.878 showing a relatively flat distribution. This demonstrated that commercial banks to a great extent are affected by technology vendor and third-party risk. The study revealed that commercial banks have diligence, contracting and monitoring procedures in place but are ineffective and inefficient, either because they are not strictly adhered to or are not up-to-date or both. Banks end up dealing with untrustworthy technology vendors and third-parties leading to financial losses.

4.5 Correlation Analysis

This section is a presentation of the correlation results involving information technology risk and Kenyan commercial banks. The results of the analysis are as shown in Table 4.3 and are presented in form of a correlation matrix.

Table 4.3: Correlation Matrix

	ROA	Strategic Risk of IT	Cybersecurity and Incidence Response Risk	IT Resiliency and Continuity Risk	Technology Vendor and Third-party Risk
ROA	1				
Strategic Risk of IT	-.124	1			
Cybersecurity and Incidence Response Risk	-.028	.296	1		
IT Resiliency and Continuity Risk	.008	-.143	.580**	1	
Technology Vendor and Third-party Risk	.158	-.088	-.170	-.103	1

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

Source: Research Findings (2018)

Pearson correlation is an important tool in evaluating the relationship between variables. The correlation matrix is important in testing the linear relationship that exist between the variables. As shown in the table 4.3, the findings derived from the study is that there exists a negative correlation between strategic risk of IT and the banks performance in financial perspective as correlation coefficient, r=-0.124. The study found that there is a negative correlation between cybersecurity and incidence response risk and the banks performance in financial perspective as correlation coefficient, r=-0.028. The study established that there exist a positive correlation IT resiliency and continuity risk and the banks performance in financial perspective as correlation coefficient, r=0.008. However, the positive correlation is weak since the correlation coefficient value is tending towards zero. The study further found a positive correlation between technology vendor and third-party risk and the banks performance financially as correlation coefficient, r=0.158. The positive correlation is also weak.

4.6 Regression Analysis

Results obtained through regression analysis encompass the model summary, analysis of variance (ANOVA) and the summary of the regression coefficients.

4.6.1 Model Summary

Table 4.4: Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.520[a]	.271	.185	.0017530

a. Predictors: (Constant), Strategic Risk of IT, Cybersecurity and Incidence Response Risk, IT Resiliency and Continuity Risk, Technology Vendor and Third-Party Risk,
b. Dependent Variable: ROA

Source: Research Findings (2018)

Adjusted R Square is referred to as coefficient of determination and was used in the study as an indicator of the level the financial performance varied with the variation in information technology risk. From table 4.4 above, the value of the adjusted R^2 is 0.271. The implication here is that there is a significant variation of 27.1%of level of financial performance varied with variation in information technology risk with a 95% confidence level. Therefore, technology vendor and third-party risk, strategic risk of IT, IT resiliency and continuity risk, cybersecurity and incidence response risk explain 27.1% variation in the performance of the Kenyan banks under study in financial perspective while 72.9% variation in financial performance is attributed to other factors as well as the error term.

4.6.2 Analysis of Variance

The results of the study obtained by the ANOVA are as shown in Table 4.5 below.

Table 4.5: ANOVA

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.000	4	.000	3.157	.026[b]
	Residual	.000	34	.000		
	Total	.000	38			

a. Dependent Variable: ROA
b. Predictors: (Constant), Technology Vendor and Third-Party Risk, Strategic Risk of IT, IT Resiliency and Continuity Risk, Cybersecurity and Incidence Response Risk

Source: Research Findings (2018)

Table 4.3 above shows ANOVA results which indicate that the relationship between information technology risk and the financial performance of commercial banks is significant since the calculated P-value is 0.026, a value which is less compared to the significance value of 0.05.

4.6.3 Regression Coefficients

Table 4.6: Regression Coefficients

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.007	.002		3.407	.002
	Strategic Risk of IT	-.001	.000	-.363	-2.163	.038
	Cybersecurity and Incidence Response Risk	.001	.000	.331	1.618	.115
	IT Resiliency and Continuity Risk	-.001	.000	-.504	-2.565	.015
	Technology Vendor and Third-Party Risk	-.001	.000	-.332	-2.234	.032

a. Dependent Variable: ROA

Source: Research Findings (2018)

From table 4.6 above, there is a negative (B=-0.001) and significant relation between strategic risk of IT and commercial banks performance in financial perspective. The results indicated a positive (B=0.001) but insignificant relation between cybersecurity and incidence response risk and performance of commercial banks in financial perspective. The findings further established a negative (B=-0.001) and significant relation between IT resiliency and continuity risk and the banks' financial performance. The study further found a negative (B=-0.001) and significant relation between technology vendor and third-party risk and financial performance of commercial banks in Kenya. Thus, from the study the regression equation obtained took the form of

$$Y= 0.007 – 0.001X1 + 0.001X2 – 0.001X3 - 0.001X4 + \mu$$

4.7 Interpretations of the Findings

The study found a significant negative relationship between strategic risk of IT and financial performance of commercial banks. This implies that a unit increase in strategic risk of IT significantly reduce the Kenyan banks performance in financial perspective by 0.001 units thus there is an inverse relationship between strategic risk of IT and the Kenyan banks performance in financial perspective.

The study found an insignificant positive relationship between cybersecurity and incidence response risk and the Kenyan banks performance in financial perspective. The implication is that a unit increase in cybersecurity and incidence response risk positively but insignificantly affect the financial performance of commercial banks by 0.001 units thus there is a direct relationship between cybersecurity and incidence response risk and the Kenyan banks performance in financial perspective.

The study also found a significant negative relationship between IT resiliency and continuity risk and performance of Kenyan commercial banks in financial terms. This means that a unit increase in IT resiliency and continuity risk negatively and significantly affect the financial performance of commercial banks by 0.001 units thus there is an inverse relationship between IT resiliency and continuity risk and performance of Kenyan commercial banks in financial terms.

The study further found a significant negative relationship between technology vendor and third-party risk and performance of Kenyan commercial banks in financial terms. This means that a unit increase in technology vendor and third-party risk significantly reduce the financial performance of commercial banks by 0.001 units thus there is an inverse relationship between technology vendor and third-party risk and performance of Kenyan commercial banks in financial terms.

The above findings from the study conform to the findings of the study by Rot (2008) who established that IT risk results in either or all of the following: failure of IT to fulfil or rather meet business requirements; inability of the IT to ensure appropriate integrity, security as well as availability; and inappropriate implementation of an IT, thus failing to work in accordance with the laid down assumptions and therefore, increasing organizational cost. The findings are also similar to those of Ahlan and Arshad (2012) whose study found that top managers acknowledge the pivotal pervasive role that IT play in organizations as well as the consequential threats that come with the use of IT hardware together with software and are detrimental to the efficiency and effectiveness of an organization. They specifically stated that IT threats lead to financial, privacy, security and data losses.

The findings are also aligned to those of Hinz (2005) who found that heavy reliance by financial institutions on IT is the major risk which can led to breakdown of single banks or entire financial center negatively impacting not only on the affected banks but also the entire economy. The findings further concurred with the study by Jowi and Abade (2016) who established that aspects of information security risk include situations where policies as well as procedures fail, poor training on the part of employees, inadequate internal audit and unguaranteed supervision of staff, and that they negatively affect the Kenyan commercial banks in terms of financial performance.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter outlines the summary of the findings of the study from chapter four, conclusions, recommendations, limitations of the study and suggested areas for further research based on the objective of the study.

5.2 Summary of the Findings

The main objective of this study was to determine the effect of information technology risk on financial performance of commercial banks in Kenya. Strategic risk of IT, cybersecurity and incidence response risk, IT resiliency and continuity risk and technology vendor and third-party risk were used as independent variables and financial performance as dependent variable. Census was conducted on the 42 commercial banks in Kenya but data was obtained from 39 commercial banks. The study used a questionnaire to collect primary data. The reliability of the questionnaire was ascertained using the Cronbach alpha coefficient where all the alpha values were above 0.7 as is recommended.

The descriptive statistics from the study established that the mean effect of strategic risk of IT, cybersecurity and incidence response risk, IT resiliency and continuity risk and technology vendor and third-party risk was 3.2, 3.8, 3.8 and 3.8 respectively. Most of the calculated mean values correspond to a scale of 4.0 in the Likert scale of the questionnaire, an indication that commercial banks in Kenya are affected by information technology risks to a great extent. Correlation analysis results established a negative correlation between strategic risk of IT and cybersecurity and incidence response risk and financial performance. However, it established weak positive

correlation between IT resiliency and continuity risk and technology vendor and third-party risk and financial performance.

The regression analysis findings established that strategic risk of IT, cybersecurity and incidence response risk, IT resiliency and continuity risk and technology vendor and third-party risk explain only 27.1% of the variation in financial performance of commercial banks in Kenya. The research study also established that the F-statistic was 3.157 and P-value of 0.026 was significant indicating that there exists a significant relation between information technology risk and banks performance in financial perspective. The study found a significant negative relationship between strategic risk of IT, IT resiliency and continuity risk and technology vendor and third-party risk and financial performance of commercial banks. The study also found an insignificant positive relationship between cybersecurity and incidence response risk and financial performance of commercial banks in Kenya.

5.3 Conclusions

The findings of the study revealed a significant negative relationship between strategic risk of IT, IT resiliency and continuity risk and technology vendor and third-party risk and financial performance of commercial banks. Therefore, the study concludes that strategic risk of IT, IT resiliency and continuity risk and technology vendor and third-party risk significantly and negatively affects performance of Kenyan commercial banks in financial perspective.

The study found a positive and insignificant relationship between cybersecurity and incidence response risk and financial performance of commercial banks. Since the descriptive statistics showed that cybersecurity and incidence response risk affects banks financial performance to a great extent, the study conclude that there is a direct

relationship between cybersecurity and incidence response risk and performance of Kenyan commercial banks in financial perspective, thus increased cases of cybersecurity and incidence response risk including cyber-attacks, breaches in data privacy and misconduct and ineffective and inefficient cyber incident response (CIR) plan affects commercial banks financial performance.

5.4 Recommendations

The study recommend that Kenyan commercial banks ought to ensure IT risk assessment prior to adopting any new technology, ensure that the policies and procedures of IT are in line with the goals and objectives of the bank and establish an IT risk committee whose responsibilities and composition are defined. This will enable the banks to alleviate and curb losses associated with strategic risk of IT.

The study recommend that commercial banks' boards should prioritize on cybersecurity and incidence response risk by putting in place access control and security protocols aligned to the banks' businesses. Kenya's commercial banks ought also to have a functioning and well-tested CIR plan which functions to protect their valuable assets against cyber-attacks, data privacy breaches and misconduct.

The study also recommend that Kenya's commercial banks should ensure timely and convenient reaction to change in IT, rigorous recovery testing plan that supports the critical processes of the bank and stringent examination of third-party resiliency and recovery capabilities before contracting. This will minimize the losses experienced by the banks as a result of IT resiliency and continuity risk.

The study further recommends that to ensure mitigation of technology vendor and third-party risk, commercial banks in Kenya should ensure that relevant and reliable information regarding contract commitments with technology vendors and third parties

is available to them prior to entering into such commitments. Banks should also ensure regular assessment of technology vendors' standard forms of assurance and due diligence to ascertain whether thy meet the bank's IT policies and standards. Operational due diligence, contracting and monitoring procedures should also not be an option to the banks.

5.5 Limitations of the Study

The study explored information technology risk and the effect it has on Kenyan commercial banks. Therefore, the study was limited to commercial banks. The study would have been extended to cover other financial institutions across different financial sectors to enhance broad-based analysis. Resource constraints, however, place the limitation. The study further generalizes its findings to all the 42 commercial banks in Kenya and not a specific one.

The use of the Likert scale questionnaire is another limitation since the respondents were only required to respond to specified and structured questions. Therefore, the qualitative views of the respondents regarding information technology risk and banks financial performance were not obtained. Lack of cooperation from the response team due to the sensitivity of the required information for the study also limited the study and the researcher had to inform them regarding the confidentiality of the obtained information and the use of such information restricted to only academics.

5.6 Suggestions for Further Research

This study focused on the effect of information technology risk on Kenyan commercial banks and their performance in financial perspective and not the whole financial sector. The study recommends further research on effect IT risk on performance of microfinance banking institutions.

The study also concentrated only on strategic risk of IT, cybersecurity and incidence response risk, IT resiliency and continuity risk and technology vendor and third-party risk and their effect on commercial banks in as far as their financial performance is concerned. The study, therefore, recommends additional research on other information technology risks in the banking industry including the risk of managing data by banks, risk involving execution of IT programs, risk of technology operations and risk of ineffective risk management. The study further make recommendation on evaluating information technology risk using qualitative views obtained by conducting interviews. This will establish an in-depth effect of information technology risk on commercial banks financial performance.

REFERENCES

Ahlan, A. R. & Arshad, Y. (2012). Information Technology Risk Management: The case of the International Islamic University Malaysia. *Journal of Research and Innovation in Information Systems, 1,* 58-67.

Andries, M., Carteau, D., Cornaggia, S., Ginolhac, P., Gruffat, C. and Le Maguer, C. (March, 2018). *IT Risk. ACPR-Information Technology Risk,* Discussion Paper.

Ayugi, W. (2016). *Is the Banking Tier System Related to the Success of Banks in Kenya*?

Barret, S. (2016). *Effects of Information Technology Risk Management on Financial Performance of Commercial Banks.*

Basel Committee on Banking Supervision, (2005). Outsourcing in Financial Services. The Joint Forum: *International Organization of Securities Commissions International Association of Insurance Supervisors C/O Bank for International Settlements*, CH-4002 Basel, Switzerland.

CBK. (January, 2013). Risk Management Guidelines.

CBK. (2018). "*Central Bank of Kenya: Commercial Banks and Mortgage Finance Institutions*." Retrieved 28 October 2018.

Chapman, C., Hopwood, A., & Shields, M. (2007). *Handbook of Management Accounting Research*. Amsterdam, NL: Elsevier.

Chenhall, R.H. (2007). *Theorising Contingencies in Management Control Systems Research*. In C. Chapman, A. Hopwood & M. Shields (Editions), *Handbook of Management Accounting Research*, Volume 1 Oxford: Elsevier.

Deloitte. (2018). *Information Technology Risks in Financial Services: What board members need to know-and do*.

De Vaus, D.A. (2001). *Research Design in Social Research*. London: SAGE.

Ehrhardt, M. and Brigham, E. (2008). *Corporate Finance: A Focused Approach (3rd ed.).* p. 131 ISBN 978-0-324-65568-1.

Harle, P., Havas, A., Kremer, A., Rona, D. and Samandari, H. (2011). *The Future of Bank Risk Management*. McKinsey Working Papers on Risk.

Hinz, D. J. (2005, January). High severity Information Technology Risks in Finance. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on* (pp. 64c-64c). IEEE.

ISO/IEC. (2008). "*Information Technology – Security Techniques-Information Security Risk Management.*" ISO/IEC FIDIS 27005:2008.

Jowi, C.O.N. and Abade, E. (June, 2016). Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya: School of Computing and Informatics, University of Nairobi (UON), Nairobi, *Kenya. American Journal of Networks and Communications,* Volume 5, Issue 3, June 2016, pages 51-59.

Kagoyire, A. & Shukla, J. (2016). Effect of Credit Management on Performance of Commercial Banks in Rwanda: A Case Study of Equity Bank Rwanda Ltd. *International Journal of Business and Management Review*, 4(4), 1-12.

Kaimba, B. et al., (2016). Achieving *Cybersecurity Resilience: Enhancing Visibility and Increasing Awareness*. Kenya Cyber Security Report 2016-Serianu Ltd. and USIU-Africa.

Kamau, P.N. (2010). *Research on Adoption of Risk Management by Commercial Banks in Kenya.* Unpublished MBA Project, School of Business, University of Nairobi.

Kenya - Chase Bank under Receivership. (2016). *Africa Research Bulletin. Economic, Financial and Technical Series*, 53(3), pp.21213B-21213C.

Kozak, K. (2015). *The Future of Asset Management; Worldwide Securities Services*. New Jersey. Morgan Stanley Publication.

KPMG. (2014). Third-party risk management.

Maina, S.M. (2012). *Business Continuity Planning as a Strategy for Building Resilience Amongst Deposit Taking Microfinance Institutions* in Kenya, University of Nairobi.

Meigs, W.B. and Others. (1978). *"Intermediate Accounting."* McGraw-Hill, New York.

Metcalf, R.W. and Titard P.L. (1976). *"Principles of Accounting,"* W.B. Sunders, (Philadelphia).

Monetary Authority of Singapore, (June 2, 2008). *Internet Banking and Technology: Risk Management Guidelines,* Version 3.0.

Murambi, K. (2016). *An Assessment of Risks of ICT Outsourcing Functions in Commercial Banks Listed in Nairobi Securities Exchange, Kenya*. School of Computing and Informatics, University of Nairobi.

Pfeiffer, M.H. (November, 2015). *Managing Technology Risks Through Technological Proficiency-Guidance for Local Government*: Issue Paper #3, Bloustein Local Government Research Center.

Press Release. (October 13, 2015). "*Imperial Bank Limited (In Receivership)" (PDF)*. Nairobi: Central Bank of Kenya. Retrieved 25 September 2018.

Rai, S. and Mohan, L. (August, 2006). Business Continuity Model: A Reality Check for Banks in India. *Journal of Internet Banking and Commerce*, vol. 11, no. 2. Accessed: http://www.arraydev.com/commerce/jibc/

Reynolds, G. (2009). *Ethics in Information Technology*, *Cengage Learning*, ISBN 978-0-538-74622-9.

Rogers, E.M. (1995). *Diffusion of Innovations*, (4th ed.). New York: The Free Press.

Rot, A. (October 22, 2008). *IT Risk Assessment: Quantitative and Qualitative Approach-Proceedings of the World Congress on Engineering and Computer Science 2008*, WCECS 2008, October 22-24, 2008, San Francisco, USA.

Ryba, M. (2005). *Analysis and Management of Information Systems Risk (In Polish)*, Ernst & Young 2005. Retrieved from http://www.mimuw.edu.pl/~sroka/archiwalne/2005ey/materialy/

Scott, W.R. (1992). *Organizations: Rational, Natural and Open Systems*. Englewood Cliffs: Prentice-Hall.

Stoneburner, G, Goguen, A. and Feringa, A. (July, 2002). SP 800-30: *Risk Management Guide for Information Technology Systems*, *Computer Security Resource Center*.

Surry, *D*.W. (1997). *Diffusion Theory and Instructional Technology*. http://intro.base.org/docs/diffusion

Svata, V. and Fleischmann, M. (2011). *IS/IT Management in Baking Sector*. University of economics, Prague, Faculty of Informatics and Statistics (svata@vse.cz); Martin Fleischmann, Czech National Bank: AOP 19(3), 2011, ISSN 0572-3043.

Taylor, F.W. (1911). The Principles of Scientific Management. New York: Harper.

Verma, E. (July 27, 2017). *Financial Performance- Understanding its Concepts and Importance*.

Wang, Q, Lai, F. and Zhao, X. (2008). "The Impact of Information Technology on the Financial Performance of Third-Party Logistics Firms in China," Supply Chain Management: *An International Journal*, Vol. 13 Issue: 2, pp. 138-150, https://doi.org/10.1108/13598540810860976

Warsame, M. (2016). *Credit Risk Management Practices and Its Impact on Banks' Financial Performance: An Empirical Study of Islamic and Conventional Banks in Kenya*. Proceedings of Business and Social Sciences Research Conference 11 - 13 April 2016, University of London, London, UK.

Weber, M. (1946). *From Max Weber: Essays in Sociology*. Gerth, H.H. & Mills, C.W., Editions, New York: Ox-ford University Press.

Whitman, M.E. and Mattord, H. (2005). *Principles of Information Security*. Boston: Course Technology.

Williamson, O.E. (1985). *The Economic Institutions of Capitalism* (Sage Free Press, New York).

Yount, R. (2006). *Research Design and Statistical Analysis for Christian Ministry: Populations and Sampling*, ©4th ed. 2006.

APPENDICES

Appendix I: Questionnaire

Dear respondent,

This questionnaire aims at examining **the effect of information technology risk in the financial performance of Kenyan commercial banks**. The research is purely academic in nature and any information obtained from this questionnaire will be confidential. We shall appreciate your cooperation and support.

Please **tick** and **fill** where appropriate

Section A: Background Information

1. Name of the Commercial Bank.....……
2. Position: Chief Information officer ( ) Chief Risk Officer ( ) Chief Technology Officer IT Director ( ) Systems Administrator ( ) Business Partner ( ) others, specify……

Section B: Strategic Risk of IT

3. To what extent does your organization undertake the below strategies to ensure that the organization is protected from strategic risk of IT?

   Not at all 2. To a little extent 3. To a moderate extent 4. To a great extent 5. To a very great extent

Strategic Risk of IT	**1**	**2**	**3**	**4**	**5**
The bank undertakes an IT risk assessment before adopting any new technology					
The bank's IT policies and procedures are consistent with the bank's goals and objectives					

The bank optimally utilizes IT resource capacity lowering its capital costs and increasing profit margins					
he bank's IT department has IT risk committee with define responsibilities and composition					

Section C: Cybersecurity and Incidence Response Risk

4. To what extent does your organization undertake the below cybersecurity and incidence response measures to ensure that the organization is protected from cybersecurity and incidence response risk?

   Not at all 2. To a little extent 3. To a moderate extent 4. To a great extent 5. To a very great extent

Cybersecurity and Incidence Response Risk	**1**	**2**	**3**	**4**	**5**
The bank's board prioritizes on cybersecurity and incidence response					
The bank undertakes to protect its most valuable assets from cyber-attacks, data privacy breaches and misconduct					
The bank's access controls and security protocols operate in tandem with the bank's businesses					
The bank has a functioning and well-tested CIR plan in place					

Section D: IT Resiliency and Continuity Risk

5. To what extent does your organization undertake the below IT resiliency and continuity measures to ensure that the organization is protected from IT resiliency and continuity risk?

   Not at all 2. To a little extent 3. To a moderate extent 4. To a great extent 5. To a very great extent

IT Resiliency and Continuity Risk	1	2	3	4	5
The bank's structure conveniently allows timely reaction to a change in IT					
The bank has a process for tracking of IT implementation and modification in case of technological changes					
The bank has a rigorous recovery testing plan which supports the critical processes of the bank					
The bank carefully examines and understands third-party resiliency and recovery capabilities before contracting					

Section E: Technology Vendor and Third-Party Risk

6. To what extent does your organization undertake the below technology vendor and third-party relations measures to ensure that the organization is protected from technology vendor and third-party risk?

   Not at all 2. To a little extent 3. To a moderate extent 4. To a great extent 5. To a very great extent

Technology Vendor and Third-Party Risk	1	2	3	4	5
The bank has relevant and reliable information about contract commitments entered with technology vendor and third parties					
The bank engages in information sharing with technology vendors and third parties					
The bank regularly assess the technology vendors' standard forms of assurance as well as their due diligence					
The bank has an operational due diligence, contracting and monitoring procedures against its third parties					

Thank you for your support.

Appendix II: List of Licensed Commercial Banks in Kenya

1. ABC Bank
2. Bank of Africa
3. Bank of Baroda
4. Bank of India
5. Barclays Bank of Kenya
6. Chase Bank of Kenya
7. Citibank
8. Commercial Bank of Africa
9. Consolidated Bank of Kenya
10. Cooperative Bank of Kenya
11. Credit Bank
12. Development Bank of Kenya
13. Diamond Trust Bank
14. Dubai Islamic Bank
15. Eco-bank Kenya
16. Equity Bank
17. Family Bank
18. First Community Bank
19. Guaranty Trust Bank Kenya
20. Guardian Bank
21. Gulf African Bank
22. Habib Bank A.G Zurich
23. Housing Finance Company of Kenya
24. I&M Bank

25. Imperial Bank of Kenya
26. Jamii Bora Bank
27. Kenya Commercial Bank
28. Mayfair Bank
29. Middle East Bank Kenya
30. National Bank of Kenya
31. NIC Bank
32. Oriental Commercial Bank
33. Paramount Universal Bank
34. Prime Bank Kenya
35. SBM Bank Kenya Limited
36. Sidian Bank
37. Spire Bank (formerly **ECB**)
38. Stanbic Bank Kenya
39. Standard Chartered Kenya
40. Trans-National Bank Kenya
41. United Bank for Africa
42. Victoria Commercial Bank

Appendix III: Classification of Commercial Banks in Kenya (Tier System)

Tier 1	Tier 2	Tier 3
1. Cooperative Bank of Kenya	1. Family Bank	1. Jamii Bora Bank
2. Kenya Commercial Bank (KCB)	2. I&M Bank	2. ABC Bank
3. Equity Bank	3. NIC Bank	3. Credit Bank
4. Barclays Bank	4. Diamond Trust Bank	4. Paramount Universal
5. Commercial Bank of Africa	5. Bank of Africa	5. Consolidated and Development Bank
6. Standard Chartered Bank	6. Housing Finance	6. Fidelity Bank
	7. Eco-bank	7. Equatorial Commercial Bank (currently **Spire Bank**)
	8. Prime Bank	8. Giro Bank
	9. Bank of Baroda	9. Guardian Bank
	10. CFC Stanbic Bank	10. Middle East Bank
	11. Citibank	11. Oriental Commercial Bank
	12. Guaranty Trust bank	12. Paramount Universal Bank
	13. National Bank	13. Trans-National Bank
	14. Bank of India	14. Victoria Bank
		15. First Community Bank
		16. Habib A.G Zurich Bank
		17. Habib Bank
		18. Gulf Africa
		19. Sidian Bank
		20. UBA Bank
		21. Consolidated Bank
		22. Development Bank

Appendix IV: Secondary Data Collection Form

School Name: ……...……..

Department: ……...

Student Name: …… Faculty: ……....

Supervisor: …….. Submission Date: …….....

Title and Description

Title:

Effect of Information Technology Risk on Financial Performance of Commercial Banks in Kenya.

Description:

To determine the effect of information technology risk on financial performance of commercial banks in Kenya.

Description of the Method Adopted for Secondary Data Collection

- Data collected will only be from secondary sources.
- The method is quantitative where financial statements of the commercial banks will be used.
- Financial statements will be obtained from the internet, specifically websites of the various commercial banks as well as the CBK website.
- Data of both net incomes and total assets of the various commercial banks will be compiled and recorded.
- The data will be used to obtain ROA.

Rationale behind Choosing of the Method

- The background information relating to both net incomes and total assets of commercial banks can be easily and conveniently found in their respective websites and the CBK website.
- Compared to the traditional method where we can manually and physically seek financial statements from the respective banks, internet speeds up the access of the information.

Chronological Progress of Secondary Data Collection

Date **Day/Month/Year**	**Major Work to be Done**	**Achievements and Difficulties Expected**
Nov 5, 2018	Collect information for the data required from the financial statements (net incomes and total assets).	Background knowledge on such items as net incomes and total assets becomes necessary
Nov 6, 2018	Designing a table that information on net incomes and total assets will be manually fed	The table will provide an organized framework of calculating ROA for each bank.
Nov 7, 2018- Nov 8, 2018	Data mining where information (net incomes and total assets) from the particular websites are obtained.	Likelihood of feeding wrong entries of data in the designed table. Due care and vigilance therefore becomes paramount here to enhance accuracy.
Nov 9, 2018- Nov 12, 2018	Organizing, contextualizing and analysing the collected data	The data exist in table form, hence, makes it easy for analysis and subsequent correlation with data from the administered questionnaires.

Appendix V: Financial Performance Data

No.	Bank	Year	Net Income (Ksh. M)	Total Assets (Ksh. M)	ROA
1.	ABC Bank	2017	203	24,804	0.0082
		2016	222	22,422	0.0099
		2015	355	22,058	0.0161
		2014	319	21,439	0.0149
		2013	578	19,639	0.0290
2.	Bank of Africa	2017	35	54,191	0.0006
		2016	(16)	55,996	-0.0003
		2015	(1,434)	69,280	-0.0207
		2014	204	62,212	0.0033
		2013	1,028	52,683	0.0200
3.	Bank of Baroda	2017	5,053	96,132	0.0526
		2016	3,876	82,907	0.0467
		2015	2,486	68,178	0.0365
		2014	2,695	61,945	0.0435
		2013	2,505	52,022	0.0480
4.	Bank of India	2017	2,675	56,631	0.0472
		2016	2,185	47,815	0.0457
		2015	1,470	42,146	0.0349
		2014	1,284	34,370	0.0374
		2013	1,253	30,721	0.0410
5.	Barclays Bank	2017	10,006	271,682	0.0368
		2016	10,440	259,498	0.0402
		2015	12,074	241,153	0.0501
		2014	12,294	226,043	0.0544
		2013	11,921	207,010	0.0580
6.	Citibank	2017	6,373	98,232	0.0649
		2016	6,033	103,324	0.0584
		2015	5,577	88,147	0.0633
		2014	4,145	79,398	0.0522
		2013	4,984	71,243	0.0700
7.	Commercial Bank of Africa	2017	7,189	229,525	0.0313
		2016	7,593	210,878	0.0360
		2015	6,227	198,484	0.0314
		2014	4,522	175,809	0.0257
		2013	4,464	124,882	0.0360
8.	Consolidated Bank	2017	(439)	13,456	-0.0326
		2016	(277)	13,918	-0.0199
		2015	49	14,136	0.0035
		2014	(274)	15,077	-0.0182
		2013	(142)	16,779	-0.0080
9.	Cooperative Bank	2017	16,502	382,830	0.0431
		2016	18,024	349,998	0.0515
		2015	14,073	339,550	0.0414
		2014	12,515	282,689	0.0443
		2013	10,705	228,874	0.0470
10.	Credit Bank	2017	179	14,465	0.0124
		2016	158	12,202	0.0130

		2015	(179)	10,287	-0.0174
		2014	(90)	8,865	-0.0102
		2013	72	7,309	0.0100
11.	Development Bank	2017	58	16,320	0.0035
		2016	95	16,418	0.0058
		2015	178	16,943	0.0105
		2014	318	16,954	0.0188
		2013	274	15,581	0.0180
12.	Diamond Trust Bank	2017	8,228	270,082	0.0305
		2016	8,876	244,124	0.0364
		2015	7,055	190,948	0.0369
		2014	6,307	141,176	0.0447
		2013	5,566	114,136	0.0490
13.	Dubai Islamic Bank	2017	(839)	2,610	-0.3215
		2016	-	-	-
		2015	-	-	-
		2014	7	3,502	0.0021
		2013	16	2,927	0.0050
14.	Eco-bank	2017	(1,434)	53,456	-0.0268
		2016	(2,889)	47,124	-0.0613
		2015	93	52,427	0.0018
		2014	(499)	45,934	-0.0109
		2013	(1,231)	36,907	-0.0330
15.	Equity	2017	23,086	406,402	0.0568
		2016	22,778	379,749	0.0600
		2015	22,388	341,329	0.0656
		2014	20,112	277,116	0.0726
		2013	18,233	238,194	0.0770
16.	Family Bank	2017	(1,371)	69,051	-0.0199
		2016	633	69,432	0.0091
		2015	2,883	81,190	0.0355
		2014	2,618	61,813	0.0424
		2013	1,758	43,501	0.0400
17.	First Community Bank	2017	216	17,360	0.0125
		2016	(41)	14,962	-0.0028
		2015	11	14,613	0.0007
		2014	102	15,278	0.0067
		2013	200	11,305	0.0180
18.	Guaranty Trust Bank	2017	241	27,628	0.0087
		2016	659	29,619	0.0223
		2015	547	29,374	0.0186
		2014	687	32,992	0.0208
		2013	413	25,638	0.0160
19.	Guardian Bank	2017	228	15,803	0.0144
		2016	302	14,705	0.0205
		2015	329	14,609	0.0225
		2014	378	14,571	0.0259
		2013	384	12,835	0.0300
20.	Gulf African Bank	2017	254	31,360	0.0081
		2016	754	27,156	0.0278
		2015	1,093	24,714	0.0442
		2014	615	19,754	0.0311
		2013	434	16,054	0.0270

21.	Habib Bank A.G Zurich	2017	409	18,708	0.0219
		2016	622	17,033	0.0365
		2015	510	14,440	0.0353
		2014	643	12,147	0.0529
		2013	474	11,009	0.0430
22.	HFC Limited	2017	393	62,127	0.0063
		2016	1,445	68,085	0.0212
		2015	1,737	68,809	0.0252
		2014	1,285	60,491	0.0212
		2013	1,213	46,755	0.0260
23.	I&M Bank	2017	7,516	183,953	0.0409
		2016	8,651	164,116	0.0527
		2015	8,367	147,846	0.0566
		2014	7,749	137,299	0.0564
		2013	6,060	110,316	0.0550
24.	Jamii Bora Bank	2017	(762)	12,851	-0.0593
		2016	(490)	15,724	-0.0312
		2015	36	16,782	0.0022
		2014	96	13,118	0.0073
		2013	90	7,010	0.0130
25.	KCB	2017	27,472	555,630	0.0494
		2016	28,482	504,778	0.0564
		2015	23,445	467,741	0.0501
		2014	22,362	376,969	0.0593
		2013	17,746	323,312	0.0550
26.	Middle East Bank	2017	(41)	5,121	-0.0081
		2016	(101)	5,234	-0.0193
		2015	43	5,678	0.0075
		2014	76	5,937	0.0128
		2013	81	5,766	0.0140
27.	NBK	2017	740	109,942	0.0067
		2016	162	115,114	0.0014
		2015	(1,684)	125,295	-0.0134
		2014	2,332	122,865	0.0190
		2013	1,779	92,493	0.0190
28.	NIC Bank	2017	5,676	192,817	0.0294
		2016	5,926	161,847	0.0366
		2015	6,260	156,762	0.0399
		2014	6,081	137,087	0.0444
		2013	5,221	112,917	0.0460
29.	Oriental Bank	2017	116	10,577	0.0110
		2016	36	9,920	0.0036
		2015	42	8,496	0.0049
		2014	84	7,858	0.0107
		2013	178	7,007	0.0250
30.	Paramount Bank	2017	96	9,541	0.0101
		2016	105	9,427	0.0111
		2015	169	10,526	0.0160
		2014	137	10,402	0.0132
		2013	99	8,029	0.0120
31.	Prime Bank	2017	1,977	76,438	0.0259
		2016	2,336	65,338	0.0357
		2015	2,593	65,001	0.0399

		2014	2,298	54,918	0.0418
		2013	1,893	49,461	0.0380
32.	Sidian Bank	2017	(633)	19,302	-0.0328
		2016	62	20,875	0.0030
		2015	520	19,107	0.0272
		2014	-	-	-
		2013	-	-	-
33.	Spire Bank	2017	(1,576)	11,148	-0.1414
		2016	(968)	13,802	-0.0701
		2015	(655)	14,470	-0.0453
		2014	(461)	16,589	-0.0278
		2013	152	15,562	0.0100
34.	SBM Bank	2017	(361)	11,745	-0.0307
		2016	-	-	-
		2015	-	-	-
		2014	-	-	-
		2013	-	-	-
35.	Stanbic Bank	2017	5,599	239,408	0.0234
		2016	6,910	204,895	0.0337
		2015	7,077	198,578	0.0356
		2014	7,391	171,347	0.0431
		2013	7,005	170,726	0.0410
36.	Standard Chartered	2017	9,510	285,125	0.0334
		2016	12,764	250,274	0.0510
		2015	8,974	234,131	0.0383
		2014	14,300	222,636	0.0642
		2013	13,316	220,524	0.0600
37.	Trans-National Bank	2017	54	10,295	0.0052
		2016	160	10,465	0.0153
		2015	252	10,533	0.0239
		2014	191	10,240	0.0186
		2013	225	9,658	0.0230
38.	UBA Kenya Bank	2017	14	6,505	0.0021
		2016	50	5,601	0.0089
		2015	(304)	7,781	-0.0391
		2014	(331)	4,756	-0.0697
		2013	(278)	3,710	-0.0750
39.	Victoria Commercial Bank	2017	849	25,985	0.0327
		2016	796	22,403	0.0355
		2015	677	20,020	0.0338
		2014	635	17,244	0.0368
		2013	586	13,644	0.0430

Source: CBK, Bank Supervision Annual Report