

CLOUD COMPUTING IN THE KENYAN BANKING INDUSTRY

RASHID JAMES MUNGAI

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

NOVEMBER 2012

DECLARATION

This research project is my original work and has not been submitted for a degree in any other University.

Signature_____ Date_____

Rashid James Mungai

D61/75722/2009

This research project has been submitted for examination with my approval as the university supervisor.

Signature_____ Date_____

Joel K. Lelei

Lecturer, School of Business, University of Nairobi

DEDICATION

To my parents Professor David N. Mungai and Rukia Mwari Kibaya, your encouragement, love and “sacrifice” made it possible for me to hope for tomorrow.

ACKNOWLEDGEMENT

I would like to give special thanks to my supervisor Joel K. Lelei for his professional guidance offered tirelessly during the initial stages of this project and seeing it through. I am grateful to the Executive Director of Neptune Software Group, Edward Makole for the study leave that allowed me to attend classes unfailingly as well as work on my project. Thank you Ronald Nyangau (University of Nairobi) for the invaluable assistance you have provided during the process of data collection and analysis. I am also grateful to all my friends at University of Nairobi and colleagues at Neptune Software. Last but not least I would like to thank my siblings for all the support they gave me to see this through.

ABSTRACT

Cloud Computing refers to the offering of dynamically provisioned computing services comprising of a mix of application platforms and or hardware capacity to users through a network of geographically disbursed systems. The service is typically offered through geographically disbursed and large data centers based on well-defined service level agreements. Given that firms are adopting this technology due to the benefits it provides such as cost savings, reliability and scalability, the objectives of the study were to establish the extent of Cloud Computing adoption in the Kenyan banking industry, its benefits, risks and mitigation strategies for the risks.

The study was a census of the 44 commercial banks operating in Kenya. Primary data was collected using a questionnaire administered to ICT managers or their equivalents who could provide the required data, out of the 44 banks only 40 responded. The quantitative data collected was analyzed using means, percentages and frequencies; in addition factor analysis was used to determine the suitability of the mitigation strategies. The results were presented in frequency tables to facilitate comparisons and graphs to identify any underlying trends.

The study found out that 57% of the respondents were male, 60% of the respondents were in their middle ages, 62% of the respondents had attained degree level of education while 8% of the respondents had attained post graduate level, 52% of the respondents were ICT managers and 60% of the respondents were from banks whose total assets lied between 10 and 40 billion. 90% of the banks that responded had not adopted Cloud Computing but

they recognized the benefits it offers such as minimizing IT costs both upfront costs as well as ongoing maintenance costs. Despite these benefits banks identified risks such as security, vendor lock-in, loss of governance and compliance issues as reasons as to why they were reluctant to adopt Cloud Computing but agreed that auditing vendors of Cloud services and coming up with standard protocols on how the technology can be made safe for use by banks as some of the mitigation strategies that can be used against the risks.

The study concludes that banks in Kenya are yet to fully adopt Cloud Computing despite its well documented benefits of cost savings, business continuity, business agility and focus. This is as a result of all the risks that banks face when adopting Cloud Computing. The study concludes that banks need to build their confidence in the technology by proactively taking steps to put in place a framework with all stakeholders that would push for Cloud Computing adoption within the industry.

Table of Contents

DECLARATION	ii
DEDICATION	iii
ACKNOWLEDGEMENT	iv
ABSTRACT.....	v
LIST OF TABLES	x
LITS OF FIGURES	xi
CHAPTER ONE: INTRODUCTION.....	1
1.1 Background of the Study.....	1
1.2 Kenyan Banking Industry.....	6
1.3 Statement of the Problem	8
1.4 Research Objectives	9
1.5 Value of the Study.....	10
CHAPTER TWO: LITERATURE REVIEW.....	11
2.1 Introduction	11
2.2 Cloud Computing	11
2.3 Cloud Computing Service Models	12
2.4 Benefits of Cloud Computing	14
2.5 Cloud Computing Risks	16
2.3.1 Policy and Organizational Risks.....	16
2.3.2 Technical Risks.....	18
2.3.3 Legal Risks.....	20
2.6 Mitigation Strategies	23
2.5.1 Audit Controls.....	23

2.5.2 Policies and Procedures	24
2.5.3 Service level Agreements	24
2.5.4 IT Governance	26
2.7 Conceptual Framework	27
CHAPTER THREE: RESEARCH METHODOLOGY	29
3.1 Introduction	29
3.2 Research Design.....	29
3.3 Population and Sample Size.....	29
3.4 Data Collection.....	30
3.5 Data Analysis	30
CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION	32
4.1 Introduction	32
4.2 Demographics.....	32
4.2.1 Gender.....	32
4.2.2 Age.....	33
4.2.3 Level of Education.....	34
4.2.4 Profession.....	34
4.2.5 Bank Size	35
4.2.6 Shareholding Information	36
4.3 Extent of Cloud Computing Adoption	37
4.4 Benefits of Cloud Computing	39
4.5 Cloud Computing Risks	41
4.6 Mitigation Strategies	44
CHAPTER FIVE: SUMMARY CONCLUSION AND RECOMMENDATIONS.....	47
5.1 Summary	47

5.2	Summary of the Findings	47
5.2.1	Demographic Information.....	47
5.2.2	Extent of Cloud Computing Adoption.....	48
5.2.3	Benefits of Cloud Computing.....	48
5.2.4	Cloud Computing Risks.....	48
5.2.5	Mitigation Strategies.....	49
5.3	Conclusion.....	49
5.4	Recommendations	50
5.5	Limitations of the Study.....	51
5.6	Recommendations for Further Study	51
	References.....	52
	Appendices.....	58
	Appendix 1: Letter of Introduction.....	58
	Appendix 2: Questionnaire	59
	Section A: Individual and Organizational Bio Data	59
	Section B: Extent of Cloud Computing Adoption	61
	Section C: Benefits of Cloud Computing	62
	Section D: Cloud Computing Risks.....	63
	Section E: Mitigation Strategies	64
	Appendix 3: List of Commercial Banks in Kenya.....	66

LIST OF TABLES

Table 4.1	Results of Gender analysis	22
Table 4.2	Results of Age analysis	23
Table 4.3	Results of Level of Education analysis	23
Table 4.4	Results of Profession analysis	24
Table 4.5	Results of Bank Size analysis	24
Table 4.6	Results of Shareholding Information analysis	25
Table 4.7	Extent of Cloud Computing Adoption	25
Table 4.8	Benefits of Cloud Computing	26
Table 4.9	Cloud Computing Risks	28
Table 5.0	Mitigation Strategies	30

LITS OF FIGURES

Figure 1: Conceptual Framework	28
--------------------------------------	----

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Over the years many organizations have invested in massive in-house computing capacities and specialized Information Technology (IT) staff around the world in order to support their primary business processes or to achieve a competitive advantage. Information Technology creates competitive advantage by giving companies new ways to outperform their rivals (Porter & Millar, 1985). To gain competitive advantage over its rivals, a company must either perform these activities at a lower cost or perform them in a way that leads to differentiation and premium price (Porter & Millar, 1985). Nowadays organizations are making use of IT to operate more efficiently and help to reduce the overall costs. The concept of outsourcing has contributed to this development by transferring entire business functions to an external service provider (Van Elst, 2010).

A phenomenon taking center stage in outsourcing is Cloud Computing. Cloud Computing is defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as services over the Internet (Furht & Escalante, 2010). This means that more and more ICT services (applications and technology) are outsourced to external vendors over the Web, which eventually will lead to a change in the traditional business model where IT is in-house organized to a virtual enterprise. This virtual enterprise, based on mainly Cloud services, could be the future perspective

(Gewald & Dibbern, 2009). In the concept of Cloud Computing, clouds are a large pool of easily usable and accessible virtualized resources such as hardware, development platforms and/or services. These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization.

There are generally three types of IT services which an organization can send into a cloud environment; these are Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). Platform as a Service is where users are offered application programming interfaces over the internet as opposed to creating fully-blown applications for example Google App Engine, Software as a Service is where applications are delivered through a browser to thousands of customers using a multiuser architecture for example Internet Banking and Infrastructure as a Service is which is the delivery of computer infrastructure as a service for example Amazon Web Service (Feuerlicht & Govardhan, 2009).

A large number of small to medium sized organizations have implemented a service model of Cloud Computing and have indicated that the benefits of Cloud architecture outweighs the risks, compared to large organizations (Van Elst, 2010). This has been attributed to the fact that smaller companies do not have the luxury of huge funds and Cloud Computing allows them to handle the IT budget in a more flexible way (Van Elst, 2010). Telecommunication companies have continually adopted Cloud Computing to a large extent an example being Safaricom who run their mobile money transfer application M-Pesa on a Cloud. Cloud Computing can offer banks a number of benefits for example

turning a large up front capital expenditure to a smaller on-going operational cost (Sriram, 2011). Cloud computing principally facilitates the conversion of Capital Expenditure (CAPEX) to Operating Expenditure (OPEX) as resources are rented rather than bought, thereby reducing the corporate opportunity cost of investment decision in IT (KPMG, 2009). Cloud service vendors are utilizing the concept of “Utility Computing”. This means, just like the principle of electricity that you pay for the resources you actually use (Radhakrishnan, Zu, & Grover, 2006).

Another benefit is, with Cloud Computing the provider is responsible for managing the technology giving banks a higher level of data protection, fault tolerance and disaster recovery ensuring there is business continuity at all times (Sriram, 2011). The flexibility of cloud-based operating models allows banks experience shorter development cycles for new products. This supports a faster and more efficient response to the needs of banking customers (Sriram, 2011). Cloud computing also allows banks to move non-critical services to the cloud including software patches, maintenance and other computing issues so that they can focus on the business of Financial Services, not IT (Sriram, 2011).

Organizations using Cloud Computing transfer their services to a virtual environment that reduces energy consumption and carbon footprint that comes from setting up a physical infrastructure (Sriram, 2011). Cloud Computing provides elasticity to organizations enabling them to add or remove resources at a fine grain and with a lead time of minutes rather than weeks allowing matching of resources to workload more closely (Armbrust, et al., 2009). The organization has the benefit of higher availability compared to in-house solutions due to the increased availability of virtualized technologies that enable creation of customized

environments atop physical infrastructures (Van Elst, 2010). Organizations also have access to a variety of software applications and features through SaaS (Van Elst, 2010).

Cloud computing is expected to be one of the fastest-growing technologies in the coming years. Business applications will be the largest market for cloud services spending, with a gradual transition from on-premise to cloud-based services especially for general business applications like customer relationship management (CRM) and enterprise resource planning (ERP).

Cloud Computing is easiest to adopt when there is a considerably flexible approach to phasing it in and relating it to other applications. Technology adoption has been defined as the choice to acquire and use a new invention or innovation (Hall & Khan, 2002). The determinants of new technology adoption are the benefits received by the user and the costs of adoption (Hall & Khan, 2002). In many cases these benefits are simply the difference in profits when a firm shifts from an older technology to a newer one while in the case of consumers the benefits are the increased utility from the new good or service but may also be the satisfaction of being an early adopter (Hall & Khan, 2002). There are other factors that determine the demand for new technologies and these are availability of complementary skills and inputs, the strength of the firm's relation to its customers, and the importance of network effects because of a high degree of interrelation among technologies simply because utility directly increases with the total size of the network (Hall & Khan, 2002).

Despite all the benefits Cloud Computing offers organizations, there are risks that the technology exposes organizations to. Banks are expected to enter the cloud computing arena cautiously, with no single cloud services delivery model being a silver bullet for best meeting their demanding business needs because banks must consider issues around data confidentiality, security, regulatory compliance, interoperability of standards, and quality of services (Microsoft, 2010). Cloud Computing risks can be divided into 3 categories namely policy and organizational, technical and legal risks (Betcher, 2010). A study done by the London School of Economics and Accenture reveals that IT executives are more cautious about implementing on the Cloud as opposed to business executives who are especially interested in agile and cost-effective IT solutions in the short-term (Willcocks, Venters, & Whitley, 2011), because of the several implementation challenges such as safeguarding data security as users of the cloud are concerned about the security of data outside the corporate firewall, managing the contractual relationship since Cloud Computing is a mix of outsourcing, software and leasing and very few providers meet all of the clients actual requirements making it necessary for a customer to use a mix of providers, dealing with lock-in because service providers have made it relatively costly to switch from one Cloud vendor to another and finally the challenge of managing the Cloud in terms of developing adequate management capabilities and principles for operating with Cloud services (Willcocks, Venters, & Whitley, 2011).

To ensure widespread adoption Cloud Computing, the risks discussed above need to be addressed effectively. Some of the strategies that can be used to mitigate Cloud Computing risks are establishing cloud security and data privacy standards, establishing

technical standards for clouds, certifying cloud service providers, collaboration between governments and reduction of compliance requirements, build sustainable infrastructure that can support cloud architecture (Harris & Alter, 2010). Betcher (2010) identified the following strategies to mitigate Cloud Computing risks; placing adequate audit controls, aligning the organizations IT policies and procedures with those of the vendor, defining service level agreements that suit an organizations unique requirements and other forms of IT governance (Betcher, 2010).

1.2 Kenyan Banking Industry

A bank is defined as a company which carries on or proposes to carry on banking business in Kenya but does not include the Central Bank (Central Bank of Kenya, 2011). Banking Business means accepting from members of the public of money on deposit repayable on demand or at the expiry of a fixed period or after notice, accepting from members of the public of money on current account and payment on and acceptance of cheques and the employing of money held on deposit or on current account or any part of the money by lending, investment or in any other manner for the account and at risk of the person so employing the money (Central Bank of Kenya, 2011). Banking industry is a collection of banks operating within the same environment.

A rapid shift in attitude towards cloud banking is happening within the financial services (FS) industry, according to Gartner Incorporated (Gartner, 2011). A Gartner survey found that cloud is the top priority for global FS Chief Information Officer's (CIOs) and that 39 percent of those surveyed expect that more than half of all their transactions will be supported via cloud infrastructure and software as a service (SaaS) by 2015. In Europe,

the Middle East and Africa (EMEA), 44 percent of FS CIOs expect that more than half of all their institutions' transactions will be supported via cloud infrastructure by 2015 and 33 percent of them expect that the majority of transactions will be processed via SaaS by 2015 (Gartner, 2011).

As of December 2011 Kenya had 43 licensed commercial banks and 1 mortgage finance company according to the Central Bank of Kenya (CBK) which offer a wide range of services ranging from Deposit Accounts, to extending Credit facilities, Investment Banking, Financial Planning, Custodial Services as well as 24/7 access to ones accounts through Automated Teller Machines (ATM); Mobile Banking; Online Banking. For Banks to offer these services they need to access crucial customer information that is stored in voluminous data banks. Banks have had to heavily adopt ICT in order to be customer centric in their operations as well as grow their range of products which will in turn assist them grow their customer base while reducing transactional and operational costs through automation.

Kenyan banks have experienced increased competition over the last few years from increased innovation among the players, new entrants into the market, change in regulation, economic conditions like the 2008 global financial crisis have affected the banking sector according to Price Water House Cooper (<http://www.pwc.com/ke/en/industries/banking.jhtml>, accessed on 23rd October 2012). Banks have been forced to find new efficient and effective ways of doing business in order to gain or retain competitive advantage, widen their customer base, grow their range of products and be more customer centric (Awuondo, 2008). A study done on the

commercial application of ICT in the banking sector by Awuondo listed some of the notable applications such as networked branches, ATM's, Internet Banking, Short Message Service (SMS) Banking, Mobile Banking, Electronic Bill Payment, Point of Sale (POS) Banking have been developed as a result of Banks adopting ICT(Awuondo, 2008). The continual adoption of ICT has led to the development of more sophisticated and innovative products that Banks have quickly consumed such as M-Pesa, Mobile Banking, Pesa Point (Awuondo, 2008). Technological innovation has brought several gains to the banking sector in Kenya such as enhanced customer access and awareness, cost and time effectiveness due to automation of processes, reduction of fraud levels and improved risk management, global compliance by adopting trends to provide seamless and standardized services worldwide, banks have become customer centric, convenience and wider networking. This has not been without challenges such as majority of the customers shying away from ICT related banking services due to security concerns, customers still value personalized and responsive services from their bankers, poor and or lack of technological infrastructure especially in the rural areas (Awuondo, 2008).

1.3 Statement of the Problem

Cloud computing offers Banks greater flexibility in terms of capacity, agility and costs yet banks are reluctant to embrace cloud technology wholly, the emerging trend is deployment of non-core applications such as email on the cloud (Microsoft, 2010). According to a survey done by IBM in 2010, issues like security, lack of a clear value proposition, lack of standardization, funding, security and managing complexity were major barriers to adopting Cloud Computing (IBM, 2010), this also limits the extent to which Banks adopt Cloud Computing. Harris & Alter (2010) discovered that companies

are eager to use cloud technology platforms to support important business processes but also discovered that the perceived benefits and risks from cloud computing vary more by country than by industry (Harris & Alter, 2010). Although the benefits of cloud computing are well documented and is the dominant focus for vendors and customer alike, most do not know the key IT related risks of cloud computing and the mitigation strategies, these strategies vary depending on service model that has been deployed. A study has been carried out in the United States by Betcher (2010) to identify the key public cloud computing IT related risks that should be considered by organizations and the mitigation strategies that can be used by organizations. Another study carried out by Wooley (2011) identified security risks inherent in the Cloud Computing service known as Infrastructure as a Service (IaaS) but did not go further to provide mitigation strategies for this service model.

Risks should always be understood in relation to overall business opportunity and appetite for risk (ENISA, 2009) which means depending on how Cloud Computing is utilized the inherent risks will vary from organization to organization. The research will answer the following questions: To what extent have banks in Kenya have adopted Cloud Computing? What risks does adoption of cloud computing expose a bank to? What are the most suitable mitigation strategies for these risks? What are the benefits of Cloud Computing in the Kenyan Banking Industry?

1.4 Research Objectives

With focus on the Kenyan Banking industry, the research objectives were:

- a) Determine the extent to which Cloud Computing has been adopted

- b) Establish the benefits of Cloud Computing.
- c) Establish the risks associated with Cloud Computing.
- d) Establish mitigation strategies for the risks.

1.5 Value of the Study

The study will seek to clarify that Cloud Computing risks, benefits and mitigation strategies are similar and do not vary from industry to industry. This information is beneficial to business executives and ICT managers or CIO's in particular to facilitate evaluation and mitigation of the risks associated with adopting Cloud Computing technologies. This information will also be beneficial to policy makers in the Kenyan Banking Industry to aid them in deciding research policy to develop technologies to mitigate risks; furthermore the results of this study will also assist the industry regulator decide on appropriate policy and economic incentives and legislative measures that will aid Cloud Computing adoption.

This study intends to identify the risks and assign them weight values in terms of impact on business continuity as well as offer suitable mitigation strategies for each. The study intends to equip IT security practitioners within the banking industry a framework for vetting Cloud Computing vendors objectively in order to maximize the return on investment while minimizing the risk of Cloud Computing.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

In this chapter we shall analyse relevant literature that relate to the proposed study such as definition of Cloud Computing, Cloud Computing Service models, benefits of Cloud Computing, Cloud Computing risks and mitigation strategies, previous studies done on this topic with the intent to point out areas overlooked or inadequately addressed by these studies and finally come up with the conceptual framework based on the reviewed literature that will guide the proposed study.

2.2 Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2009).The cloud promotes availability through the following characteristics; On-demand self-service where a customer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each of the service's provider; Broad Network Access where capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs); Resource Pooling where the provider's computing resources are pooled to serve multiple

consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand (Mell & Grance, 2009).

There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines; Rapid Elasticity where capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in (Mell & Grance, 2009). To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time; Measured Service where Cloud Systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service (Mell & Grance, 2009).

2.3 Cloud Computing Service Models

Cloud service models offer institutions the option to move from a capital-intensive approach to a more flexible business model that lowers operational costs. The key to success lies in selecting the right cloud services model to match business needs (Sriram, 2011).

The various models for Cloud Computing Services operations and deployment include Software-as-a-Service (SaaS) in which a cloud service provider houses the business software and related data, and users access the software and data via their web browser. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings (Christiansen, et al., 2010).

Platform-as-a-Service (PaaS) where a cloud service provider offers a complete platform for application, interface, and database development, storage, and testing, this allows businesses to streamline the development, maintenance and support of custom applications, lowering IT costs and minimizing the need for hardware, software, and hosting environments. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations (Christiansen, et al., 2010).

Infrastructure-as-a-Service (IaaS) where rather than purchasing servers, software, data center space or network equipment, this cloud model allows businesses to buy those resources as a fully outsourced service. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed

applications, and possibly limited control of select networking components like host firewalls (Christiansen, et al., 2010).

There are three ways service providers most commonly deploy clouds, Private Clouds where the cloud infrastructure is operated solely for a specific company. It may be managed by the company or a third party and may exist on or off the premises. This is the most secure of all cloud options. The second model that can be utilised is Public Clouds where the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization that sells cloud services and the third one is Hybrid Clouds where the cloud infrastructure is composed of two or more clouds (private or public) that remain unique entities but are linked in order to provide services.

2.4 Benefits of Cloud Computing

The main benefits of using Cloud Services are; there is no need for up-front infrastructure investment, investment in software licenses and no risk of unused but paid software licenses, and investment in hardware infrastructure and related maintenance and staff. Thus, capital expenditure is turned into operational expenditure. Users of a Cloud service only use the volume of IT resources they actually need, and only pay for the volume of IT resources they actually use. At the same time, they take advantage of the scalability and flexibility of a Cloud.

Cloud Computing enables easy and fast scaling of required computing resources on demand (Stanoevska-Slabeva & Wozniak, 2010); Reducing ongoing operational, upgrade

and maintenance costs by the utility model this benefit can be described as an instant result of the first one regarding the traditional IT infrastructure (Van Elst, 2010); Scaling up and down hardware, network capacity and cost based on demand (elasticity) Cloud Computing enables one to add or remove resources at a fine grain and with a lead time of minutes rather than weeks allowing matching of resources to workload much more closely (Armbrust, et al., 2009). This has everything to do with peaks in the demand (e.g. seasonal influences) for IT resources. It could be complicated for an organization to determine the ultimate number of servers needed to perform their core business. The answer is often based on a cost benefit analysis, however with the concept of Cloud Computing this should be history. Cloud Computing provides a flexible solution for this ongoing change of demand for IT resources (Van Elst, 2010).

Higher availability compared to in-house solutions through the increasing availability of Virtual Machine (VM's) is another advantage by enabling the creation of customized environments atop physical infrastructures; Access to a variety of software applications and features offered as SaaS, the technique of virtualization can be fully exploited when using the Cloud Computing model. This means that software applications can be accessed through a web interface. The consequence is that the application portfolio is getting more and more dynamic regarding changes is the business demand for instance. Applications can be added and deleted to the application portfolio in a short term. Moreover, there is hardly any maintenance (Van Elst, 2010); the real strength of Cloud Computing is that it is a catalyst for more innovation. In fact, as Cloud Computing

continues to become cheaper and more ubiquitous, the opportunities for combinatorial innovation will only grow (Hofmann, Jordan, & Brynjolfsson, 2010).

2.5 Cloud Computing Risks

Betcher (2010) identified some key reported IT-related risks that should be considered by security practitioners, these IT-related risks are classified into three categories namely policy and organizational risks, technical risks and legal risks. Mitigation strategies for the identified risks include audit controls, policies and procedures, service level agreements and other forms of governance (Betcher, 2010).

2.3.1 Policy and Organizational Risks

Policy and organizational risks are business-related IT risks that organizations may face when considering cloud computing services (Betcher, 2010). Such risk include Lock in which refers to the inability of the customer to move their data and/or programs away from a cloud computing service provider (Armbrust, et al., 2009). While customer lock-in may be attractive to cloud computing providers, customers are vulnerable to price increases, reliability problems, or even to providers going out of business (Armbrust, et al., 2009).

Loss of governance is another policy and organizational risk which has been identified as a top security risk as customers may cede control to cloud computing service providers on a number of issues that may impact their security, mission, and goals (ENISA, 2009). Businesses are vulnerable when they entrust their data to a third party (Cloud Security

Alliance, 2009). For example, non-IT personnel within the third party organization could easily violate governance policies by moving sensitive customer data into the cloud (Ryan, 2008). Cloud Computing is a “minefield” for most CIOs and IT organizations (Finnie, 2008), meaning that the impact from the loss of control may lead to the inability to comply with security requirements, a lack of confidentiality, integrity, and availability of data, a deterioration of performance and quality of service, and the introduction of compliance challenges (ENISA, 2009). Many of the leading cloud service providers do not accept responsibility for the data stored in their infrastructure, which means that they also do not accept any transference of risk (Cloud Security Alliance, 2009).

Compliance is another policy and organizational risk that organizations face due to the lack of governance over audits and industry standard assessments may leave cloud computing customers without a view into the processes, procedures, and practices of the provider in the areas of access, identity management, and segregation of duties non-inclusively leaving control risks an unknown quantity (Cloud Security Alliance, 2009). Cloud computing service providers need to be more transparent so customers can ensure they meet the appropriate rules and regulations (Betcher, 2010). Loss of business reputation is a risk in that one customer’s bad behaviour can negatively impact the reputation of the cloud as a whole (Armbrust, et al., 2009). Armbrust, et al., (2009) cite an example, hypothesizing that IP addresses by spam-prevention services may limit the types of applications that can be hosted on the cloud (p. 18). In addition, any potential legal liabilities in this example would remain with the customer, not with the cloud computing service provider (Armbrust, et al., 2009). Cloud service termination or failure:

The financial viability of Cloud Service providers is a critical issue and should be evaluated as part of initial due diligence when considering a move to a cloud computing service provider, and on an ongoing basis (Cloud Security Alliance, 2009). It is possible that in the short or medium term that some cloud computing services could be terminated due to competitive or financial pressures (ENISA, 2009). Not only can service terminations impact cloud computing customers, but downstream customers as well (ENISA, 2009).

2.3.2 Technical Risks

Technical risks are IT-related risks that have a direct, technological impact on the cloud computing systems that host customer programs and/or data (Betcher, 2010). Such risks include Availability of Service; availability of service is described as the number one obstacle to the growth of cloud computing (Armbrust, et al., 2009). Management of a cloud computing service by a single vendor creates a potential environment for a single point of failure, this is because even if the vendor has multiple data centres in different geographic regions using different network providers, the vendor may have common software infrastructure and accounting systems, or may go out of business altogether (Armbrust, et al., 2009).

Clouds are typically built on top of cheap, commodity hardware, for which failure is not uncommon. Consequently, the probability of a failure occurring during a long-running data analysis task is relatively high (Abadi, 2009). Network performance can also be a

problem for customers who are located a long geographical distance from the cloud provider (Leavitt, 2009). Network latency and propagation delay are limited by the speed of light, which is finite, and are factors that are overlooked by engineers developing cloud based applications (Smith, 2009). Without adequate network performance, applications communicating over large distances can slow down (Smith, 2009).

Another technical IT-related risk is Resource Exhaustion; since Cloud Computing Services are considered on-demand, it suggests a level of calculated risk because resources of a cloud service are allocated to statistical projections (ENISA, 2009). Although virtual machines used in Cloud Computing efficiently share CPUs and main memory, disk I/O sharing is more problematic (Armburst, et al., 2009). In particular, high performance computing applications and transactional database systems may lead to performance unpredictability and/or resource exhaustion (Betcher, 2010). With regard to data storage it is argued that availability, scalability and performance are conflicting goals as the requirements for each of these individual needs are rigorous (Youseff, et al., 2008). Data transfer bottlenecks are another technical risk, it has been observed that applications are becoming more data-intensive and expensive (Armbrust, et al., 2009). It is generally less expensive to ship large volumes of data (e.g. via FedEx), as disk capacity and cost-per-gigabyte are growing much faster than network cost-performance (Armbrust, et al., 2009). In addition to wide area network (WAN) bottlenecks, intra-cloud networking technology may be a bottleneck as well (Armbrust, et al., 2009). Although 10 Gigabit Ethernet is commonly used for the aggregation links in cloud networks, it is

currently too expensive to be used by individual servers, which often utilize slower 1 Gigabit Ethernet links (Armbrust, et al., 2009).

Finally Distributed Denial of Service (DDoS) is another technical IT-related risk, as the industry matures, to the extent that it goes toward a single interface, Cloud Computing Systems may become an easier target for attackers to threaten (Douglis, 2009). Viruses might be transmitted, or the victims of a hack attack may negatively impact other companies with data located in the same environment (Cloud Security Alliance, 2009). Criminals may also seek to extort payment from cloud computing vendors to prevent the launch of a DDoS attack that typically utilizes botnets (Armbrust, et al., 2009). Vendors however already have DDoS protection as a core competency (Armbrust, et al., 2009).

2.3.3 Legal Risks

Legal risks are the IT-related risks that are legal in nature, and can also have a negative impact on an organization using cloud computing services (Betcher, 2010). Such risks include Subpoena and e-discovery where if computer systems are confiscated by law enforcement agencies or through civil suits, the centralization of storage and shared tenancy of physical hardware imparts more risk of unwanted data disclosure to cloud computing clients (ENISA, 2009). For example the United States Patriot Act allows the government to, among other things, demand access to data stored on any computer, and if the data is stored by a third party, the data is to be handed over without the knowledge or permission of the company or person using the hosting service (Abadi, 2009). Some

businesses may not like the ability of a country to get access to their data via the court system (Armbrust, et al., 2009).

A change of Jurisdiction is another Cloud Computing legal risk where the risks may be higher for customer data that are held in multiple jurisdictions (ENISA, 2009). Although organizations may do business with a vendor down the street, data may be stored far away in a different state or country (Gatewood, 2009). Furthermore, customer data held in countries that do not respect the rule of law or international agreements could be subject to enforced disclosure or seizure (ENISA, 2009). With different jurisdictions applying their own laws, the issues and risks of data being unintentionally disclosed will grow in complexity as cloud computing is more widely adopted (Cloud Security Alliance, 2009).

Resolving these security and regulatory concerns could take years (Kaufman, 2009). In addition to data being exposed, an organization's reputation and trust with customers could be negatively impacted (ENISA, 2009). Data privacy is one of the longest standing and important concerns with cloud computing (Gatewood, 2009). In many instances, the obligations of data privacy are the responsibility of senior management (Cloud Security Alliance, 2009). Cloud Computing introduces the risk that information belonging to one organization may be resident in several locations and coexist with another organization's data (Gatewood, 2009). The type and location of data may result in a number of legal issues related to data privacy, and violations and may pertain to financial data, intellectual property, health and other information (Gatewood, 2009).Cloud Computing

Vendors give the customer little control over where data is stored and that unless the data is encrypted, it may be accessed by a third party without the customer's knowledge (Abadi, 2009).

Another legal risk that Cloud Computing poses is the risk that organizations may pay more than desired to license software on systems hosted by cloud computing service providers (Betcher, 2009). Licensing conditions, such as per-seat agreements, and online licensing checks may be unworkable in a cloud environment (ENISA, 2009). Many service providers "originally relied on open source software in part because the licensing model for commercial software is not a good match" to cloud computing (Armbrust, et al., 2009, p. 19). As a result, open source licensing models will need to remain popular and/or commercial software companies will need to change their licensing structure to better fit cloud computing (Armbrust, et al., 2009). Entering into an agreement with a Cloud Services provider without first establishing business objectives may result in significant problems (Jericho Forum, 2009). Cloud Computing is a valuable tool that is not going away, but it's a tool that needs to be understood and managed (Gatewood, 2009). Currently, there are no publicly available standards specific to cloud computing security (ISACA, 2009a). As a result, organizations considering Cloud Services need to exercise in depth due diligence prior to the execution of any agreements (Cloud Security Alliance, 2009).

2.6 Mitigation Strategies

Fortunately, there are mitigation strategies cloud computing customers can follow that may reduce the level of IT-related risks. Each of the following mitigation categories described below (audit controls, policies and procedures, service level agreements, and other forms of governance) addresses risks in each of the three IT-related cloud computing risk categories (Betcher, 2010).

2.5.1 Audit Controls

When considering a cloud based initiative or reviewing a solution already in place it is recommended you determine a vendor's internal audit process, how often it is audited by external agencies, the standards the vendor is held to, and whether or not it is open to being audited for compliance (Gatewood, 2009). Vendors rush to develop and present cloud-based solutions, they may fall short on including the necessary records management controls (Gatewood, 2009). There are challenges to conducting audits in the cloud environment, auditing cloud providers can be difficult and expensive (Cloud Security Alliance, 2009). Sponsoring an external audit may be appropriate, but a formal adopted framework and properly identified scope is necessary (Cloud Security Alliance, 2009), furthermore, some cloud providers won't allow compliance auditors on site (Rash, 2009).

To be effective in ensuring that security programs are compliant with the relevant rules and regulations, it is recommended that organizations know their legal obligations,

classify and label their data and systems, conduct an external risk assessment and conduct due diligence and consider mandating that cloud computing service providers be certified at the appropriate security level (Cloud Security Alliance, 2009). Audits of Cloud Computing implementations should focus on three elements: the client environment, the provider environment, and the cloud itself, which addresses secure communications between the client and the provider (Rai & Chukwuma, 2009).

2.5.2 Policies and Procedures

Businesses must work with legal, security, and assurance professionals to ensure that the appropriate levels of security and privacy are achieved (ISACA, 2009a). When reviewing policies and procedures related to cloud computing services it is recommended you determine the vendor's policies and procedures, and related information management approaches, are acceptable; if they are not, the data should either be moved or the vendor should make an auditable change specific to the needs of the client organization (Gatewood, 2009).

2.5.3 Service level Agreements

Given the nature of cloud computing, it is suggested that standard contract clauses with vendors may require additional review (ENISA, 2009). A Service Level Agreement is an extremely important item of documentation for both the consumer and the cloud service provider, that if used properly: identifies and defines customer needs, provides a framework for understanding, simplifies complex issues, reduces areas of conflict, encourages dialog in the event of disputes, and eliminates unrealistic expectations

(Kandukuri, Paturi, & Rakshit, 2009). Security and availability of service are two major issues that are avoided by the use of lenient SLAs (Youseff, et al., 2008). Service Level Agreements are included in the online contracts defining cloud services, but are potentially non-negotiable (Cloud Security Alliance, 2009, p. 26). If customers want to utilize the cloud service, they may have to accept the online terms with conditional clauses and privacy statements that are subject to change without notice (Cloud Security Alliance, 2009).

Service Level Agreements tend to focus on availability of services and may not explain service quality, resolution times, critical success factors, key performance indicators, or offer any recourse (Cloud Security Alliance, 2009). Customers should demand specific SLAs that cloud computing service providers must meet to satisfy required Quality of Service (QoS) requirements (Buyya, et al., 2008). Important QoS parameters that customers should consider as part of an SLA also include time, cost, reliability, and trust/security (Buyya, et al., 2008). Furthermore, QoS requirements cannot be static and should be updated over time in concert with changes in business operations (Buyya, et al., 2008). In an SLA, the delivery of new or remediated services may not be defined or mentioned (Cloud Security Alliance, 2009). Service level agreements can also be used to mitigate regulatory pressures concerning where data is processed, while specifying strict constraints on the location of Cloud Computing Service provider resources (Buyya, et al., 2008).

2.5.4 IT Governance

There are additional ways in which Cloud Computing customers can operate within a favourable environment, including establishing and promoting cloud standards with a standardized cloud application programming interface (API), customers will have an easier time migrating data between service providers (Weinhardt, Anandasivam, Blau, Borissov, Meinel, Michalk, & Stèoßer, 2009). Another form of governance of Cloud Computing is through utilizing brokers and markets (Betcher, 2010). Organizations storing information in the cloud is able to comply with all the rules and regulations it faces (Gatewood, 2009). The true federation of controls will need to expand beyond the organization itself and into the data repositories outside of the organization which currently do not exist (Gatewood, 2009). By engaging in education and developing proactive relationships, it will be more possible to identify cloud-based initiatives early and raise awareness throughout the organization (Gatewood, 2009).

In conclusion Cloud Computing is an old idea that has recently emerged as a commercial reality (Armbrust, et al., 2009). The benefits of scalability, reliability, security, ease of deployment, and ease of management for customers, traded off against worries of trust, privacy, availability, performance, ownership, and supplier persistence, still stand (Erdogmus, 2009). That is, the economies of scale and flexibility of cloud computing are both a friend and a foe from a security point of view (ENISA, 2009). Cloud Computing requires good governance, risk management, and common sense on the part of organizations (Cloud Security Alliance, 2009).

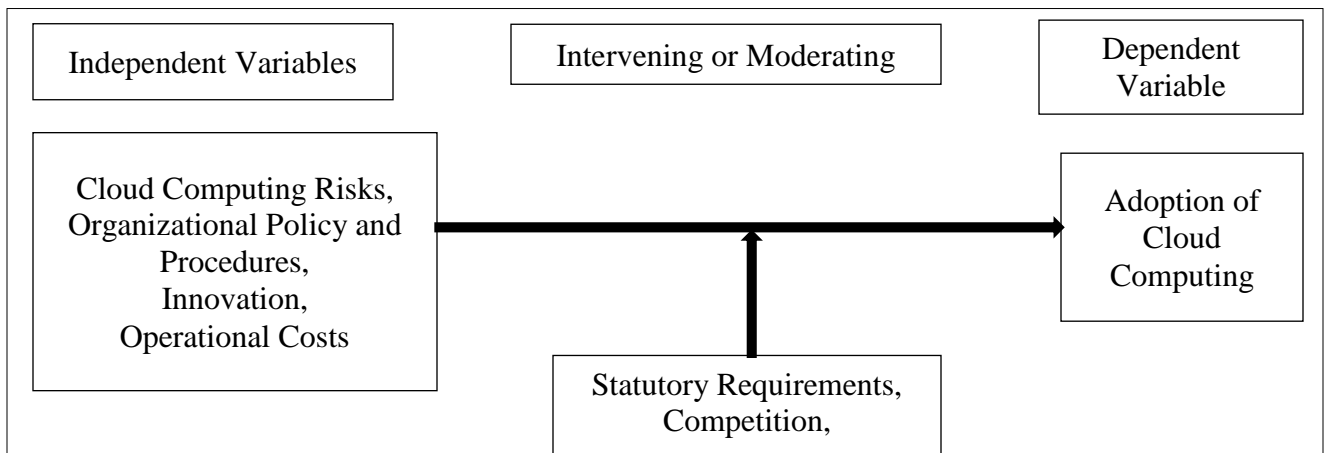
2.7 Conceptual Framework

In conclusion, a common theme in the reviewed literature is that adoption of Cloud Computing will be necessary to support various business objectives in the near future a survey conducted by Gartner found that in Europe, Middle East and Africa 44% of Financial Services CIO's expect their transactions to be supported via Cloud infrastructure. However a survey conducted by IBM highlighted issues like security, lack of a clear value proposition, lack of standardization, funding, security and managing complexity as major barriers to adopting Cloud Computing (IBM, 2010). IT executives are cautious to implement on the Cloud while their business executive counterparts would prefer the organization go cloud because of its agility and cost effectiveness (Willcocks, Venters, & Whitley, 2011).

Studies have been done to identify Cloud Computing risks such as Wooley (2011) who identified inherent risks in the Infrastructure as a Service model but did not establish mitigation strategies for this service model, while Betcher (2011) identified key IT related risks and mitigation strategies for a public cloud irrespective of the industry the organization is operating in. Banks usually operate in a controlled environment due to the sensitive nature of data they hold making their operating environment quite unique, a Bank has an obligation to its customers, shareholder's and the regulatory body which monitors and controls the industry. In order to adopt Cloud Computing banks must identify and manage the risk component of this innovation in order to ensure its obligations to various stakeholders are met. This forms the conceptual framework of this

study where the independent variables Cloud Computing risks, organizational policy and procedures, innovation as a key market differentiator and managing operational costs are key drivers for adoption of Cloud Computing in a moderating environment known as the Kenyan Banking Industry where variables like statutory requirements and fierce competition affect the adoption of Cloud Computing in Kenyan Banks as illustrated in Figure 1:

Figure 1: Conceptual Framework



CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

Research methodology documents the process of how the project was approached by defining the procedures, definitions and explanations of techniques used to collect, store, analyze and present information as part of a research process. It also describes the methods that were used by the researcher in data collection and analysis.

3.2 Research Design

The research was conducted through a survey. A survey is an attempt to collect data from members of a population in order to determine the current status of that population with respect to one or more variables (Cutler, 1991). A survey was chosen because it seeks to obtain information that describes existing phenomena by asking individuals about their perceptions, attitudes, behaviours or values (Mugenda & Mugenda, 1999).

3.3 Population and Sample Size

The target population is commercial banks that are operating in Kenya. There are 44 Financial Institutions operating in the Kenyan Banking Industry of which 43 are Commercial Banks and 1 is a Mortgage Financial Institution according to Central Bank of Kenya (www.centrabank.go.ke/financialsystem/banks/Introduction.aspx, accessed on 5th July 2012). The study will be a census.

3.4 Data Collection

This research used primary data. Data collection was through a questionnaire administered using the “drop and pick later “method. The respondents of these questionnaires were bank CIO’s or their equivalent and ICT security practitioners because they play the role in adoption of ICT by the banks.

The questionnaire consists of 5 sections namely; Section A which collected Bio Data for both individual respondents and the organization that the respondent works for. Section B collected data on the extent of Cloud Computing adoption in the Kenyan banking industry. Section C collected data on the benefits of Cloud Computing. Section D collected data on the Cloud Computing risks and Section E collected data on the suitability of the established mitigation strategies for the Cloud Computing risks.

3.5 Data Analysis

Data relating to Section A was analysed using means, percentages and frequencies. Data collected through Section B of the questionnaire was analysed using mean scores, percentages and frequencies to establish the extent of Cloud Computing adoption by Banks; this addresses objective 1 of the study. Data collected through Section C of the questionnaire was analysed using mean scores, percentages and frequencies to establish the perceived benefits of Cloud Computing in the Kenyan Banking Industry; this addresses objective 2 of the study. Data collected through Section D of the questionnaire was analysed using mean scores, percentages and frequencies to establish the risks

related to Cloud Computing in the Kenyan Banking Industry. Data collected through Section E of the questionnaire was analysed using means, percentages and frequencies to determine the suitability of various mitigation strategies and this addresses the fourth objective of the study.

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents data findings from the field, its analysis and interpretations. The data was collected through a questionnaire and analyzed using content analysis; the respondents of the questionnaires were banking CIO's or their equivalents and ICT security practitioners in Kenyan Commercial Banks. Only 40 banks responded to the questionnaire to make the response rate of the study to be 91%.

4.2 Demographics

This section concentrates on the demographic information of the respondents. The researcher was interested in knowing their gender, age, level of education, profession, organization size and the banks shareholding information. Information from this section enables the researcher to judge whether they chose the appropriate person for the study.

4.2.1 Gender

The findings of the study as shown in Table 4.1 indicate that 57.5% of the respondents were male while female respondents made the remaining 42.5%. The majority of the respondents were male.

Table 4.1 Gender

		Frequency	Percent	Cumulative Percent
Valid	Male	23	57.5	57.5
	Female	17	42.5	100.0
	Total	40	100.0	

4.2.2 Age

The findings of the study in Table 4.2 indicate that majority of the respondents are between the ages of 36 – 40 which is 60% of the respondents, the rest were either between the ages of 26 – 30 which represented 20% of the respondents or 41 – 46 years which represented 20% of the respondents also. Majority of the respondents were in their middle ages.

Table 4.2 Age Bracket

		Frequency	Percent	Cumulative Percent
Valid	26 -30 Years	8	20.0	20.0
	36 - 40 Years	24	60.0	80.0
	41 - 46 Years	8	20.0	100.0
	Total	40	100.0	

4.2.3 Level of Education

The findings of the study in Table 4.3 indicate that 62.5% of the respondents have reached graduate level, while 20% of the respondents have reached post graduate level and 17.5% only reached diploma level. The study considered the level of education as an important aspect because it helps in making informed decision and formation of opinion

Table 4.3 Level of Education

	Frequency	Percent	Cumulative Percent
Valid Diploma	7	17.5	17.5
Degree Level	25	62.5	80.0
Post Graduate Level	8	20.0	100.0
Total	40	100.0	

4.2.4 Profession

The findings of the study in Table 4.4 indicate that 52.5% of the respondents were ICT managers while 22.5% were IT Security Practitioners, 17.5% were in Banking Operations and 7.5% were Business Analysts within the bank. The research considered profession as a relevant factor because the respondent has to be knowledgeable in Cloud Computing

Table 4.4 Profession

		Frequency	Percent	Cumulative Percent
Valid	Banking Operation	7	17.5	17.5
	IT Security Practitioner	9	22.5	40.0
	Business Analyst	3	7.5	47.5
	ICT Manager	21	52.5	100.0
	Total	40	100.0	

4.2.5 Bank Size

The findings of the study in Table 4.5 indicate 80% of the respondents were from tier II banks whose total asset size lies between 10 and 40 billion Kenya shillings while 20% of the respondents are from tier I banks whose total asset size is greater than 40 billion Kenya shillings, there was no respondent from tier III whose total asset size is less than 10 billion Kenya Shillings.

Table 4.5 Bank Size

	Frequency	Percent	Cumulative Percent
Valid Between Ksh 10 Billion and Ksh 40 Billion	32	80.0	80.0
Above Ksh 40 Billion	8	20.0	100.0
Total	40	100.0	

4.2.6 Shareholding Information

The findings of the study in Table 4.6 indicate that 60% of the respondents were from locally owned banks, 15% of the respondents were from foreign owned and not locally incorporated banks, another 15% of the respondents were from banks with government participation and 10% of the respondents were from foreign but locally incorporated with partial local ownership banks.

Table 4.6 Shareholding Information

	Frequency	Percent	Cumulative Percent
Valid Foreign Owned Not Locally Incorporated	6	15.0	15.0
Foreign but Locally Incorporated with partial Local Ownership	4	10.0	25.0
Institutions with Government Participation	6	15.0	40.0
Locally Owned Institution	24	60.0	100.0
Total	40	100.0	

4.3 Extent of Cloud Computing Adoption

The first objective of the study was to determine the extent of Cloud Computing adoption in the Kenyan Banking industry. The respondents were asked to rate the extent to which Cloud Computing has been adopted in the Kenyan Banking Industry for the listed services. A numerical score of 1=No Extent; 2=Little Extent; 3=Moderate Extent; 4=Large Extent; 5=Very Large Extent was coded and used to analyze the results as shown in Table 4.7.

Table 4.7 Extent of Cloud Computing Adoption

	N	Mean	Std. Deviation
To which extent has cloud computing been adopted in point of sale (POS) in your bank	40	1.0000	.00000
To which extent has cloud computing been adopted in ATM mobile banking in your bank	40	1.0000	.00000
To which extent has cloud computing been adopted in Mobile banking in your bank	40	1.3000	.91147
To which extent has cloud computing been adopted in Internet banking in your bank	40	1.0000	.00000
To which extent has cloud computing been adopted in Customer Relationship Management banking in your bank	40	1.1000	.30382

To which extent has cloud computing been adopted in Enterprise Resource Planning in your bank	40	1.1000	.30382
To which extent has cloud computing been adopted in Core Banking [Deposits and Credit Facilities] in your bank	40	1.0000	.00000
To which extent has cloud computing been adopted in Trade-Finance in banking in your bank	40	1.0000	.00000
To which extent has cloud computing been adopted in Treasury in your bank	40	1.0000	.00000
To which extent has cloud computing been adopted in Office Email in your bank	40	1.3000	.91147

Responses in Table 4.7 indicate that POS, ATM, Internet Banking, Core Banking, Trade Finance and Treasury have a weighted mean score of 1, which means that no bank in Kenya has adopted Cloud Computing for these services. Table 4.7 also shows that Mobile Banking, Customer Relationship Management, Enterprise Resource Planning and Office Email have a mean score of 1.3, 1.1, 1.1 and 1.3 respectively which means that Cloud Computing has been adopted for these services to a small extent.

4.4 Benefits of Cloud Computing

The second objective of the study was to determine the benefits of Cloud Computing in the Kenyan Banking industry. The respondents were asked to rate the extent to which they agree their banks can benefit by adopting Cloud Computing. A numerical score of 1=No Extent; 2=Little Extent; 3=Moderate Extent; 4=Large Extent; 5=Very Large Extent was coded and used to analyze the results as shown in Table 4.8.

Table 4.8 Benefits of Cloud Computing

	N	Mean	Std. Deviation
To which extent do you agree as to the benefits that your bank could realize in Reduced up front IT Cost on adopting Cloud Computing	40	3.8500	1.14466
To which extent do you agree as to the benefits that your bank could realize in Reduced cost of maintaining IT infrastructure on adopting Cloud Computing	40	4.0000	1.01274
To which extent do you agree as to the benefits that your bank could realize in Improved communication and collaboration between individuals on adopting Cloud Computing	40	4.0250	1.02501
To which extent do you agree as to the benefits that your bank could realize in Standardized and efficient business processes on adopting Cloud Computing	40	4.2000	.96609
To which extent do you agree as to the benefits that your bank could realize in Provision of new ways to engage and interact with customers on adopting Cloud Computing	40	4.1250	.96576

To which extent do you agree as to the benefits that your bank could realize in Assured IT services with limited resources on adopting Cloud Computing	40	4.3000	.85335
To which extent do you agree as to the benefits that your bank could realize in Faster Product / Service Development on adopting Cloud Computing	40	3.9750	1.02501
To which extent do you agree as to the benefits that your bank could realize in Rapid changing of business proceeds on adopting Cloud Computing	40	3.7000	1.24447
To which extent do you agree as to the benefits that your bank could realize in Improved analytical capabilities on adopting Cloud Computing	40	3.9000	1.03280
To which extent do you agree as to the benefits that your bank could realize in Enabled processes that are not otherwise cost-effective or feasible on adopting Cloud Computing	40	4.2000	1.01779
To which extent do you agree as to the benefits that your bank could realize in Facilitation of efficient data exchange with external organizations on adopting Cloud Computing	40	4.0000	.64051
To which extent do you agree as to the benefits that your bank could realize in Establishment of uniform processes in different regions on adopting Cloud Computing	40	3.9750	.99968
To which extent do you agree as to the benefits that your bank could realize in Development of products or services that were feasible before on adopting Cloud Computing	40	4.1750	1.03497
To which extent do you agree as to the benefits that your bank could	40	4.1000	1.05733

realize in Reduced energy consumption on adopting Cloud Computing			
To which extent do you agree as to the benefits that your bank could realize in Reduced TCO on adopting Cloud Computing	40	3.8000	1.32433

Table 4.8 indicates that the mean scores for all the Cloud Computing benefits lie between 3.85 and 4.3. This means that most of the respondents agree to a large extent that banks can benefit from Cloud Computing.

4.5 Cloud Computing Risks

The third objective of the study was to determine the risks banks face in adoption of Cloud Computing in the Kenyan Banking industry. The respondents were asked to rate the extent to which their banks would face the listed risks associated with Cloud Computing. A numerical score of 1=No Extent; 2=Little Extent; 3=Moderate Extent; 4=Large Extent; 5=Very Large Extent was coded and used to analyze the results as shown in Table 4.9.

Table 4.9 Cloud Computing Risks

	N	Mean	Std. Deviation
To what extent does your bank face Vendor Lock-in risk in the adoption of Cloud Computing	40	4.4500	.74936

To what extent does your bank face Loss of Governance risk in the adoption of Cloud Computing	40	4.4500	.74936
To what extent does your bank face Compliance Challenges risk in the adoption of Cloud Computing	40	4.3500	.73554
To what extent does your bank face Loss of Business Reputation risk in the adoption of Cloud Computing	40	3.2250	1.14326
To what extent does your bank face Loss of Cloud Service termination or failure risk in the adoption of Cloud Computing	40	4.4500	.74936
To what extent does your bank face Availability of Services risk in the adoption of Cloud Computing	40	4.4500	.74936
To what extent does your bank face Resource Exhaustion risk in the adoption of Cloud Computing	40	2.9500	.71432
To what extent does your bank face Data transfer bottle necks risk in the adoption of Cloud Computing	40	2.9500	.71432
To what extent does your bank face Intercepting data in transit risk in the	40	4.4500	.74936

adoption of Cloud Computing			
To what extent does your bank face Distributed denial of service risk in the adoption of Cloud Computing	40	2.9500	.71432
To what extent does your bank face Subpoena and e-discovery risk in the adoption of Cloud Computing	40	4.4500	.74936
To what extent does your bank face Changes of jurisdiction risk in the adoption of Cloud Computing	40	4.4500	.74936
To what extent does your bank face Data Privacy risk in the adoption of Cloud Computing	40	4.3500	.73554
To what extent does your bank face Licensing risk in the adoption of Cloud Computing	40	2.6500	.48305
To what extent does your bank face Risk of legal contacts that span various jurisdictions hence difficulty in enforcement risk in the adoption of Cloud Computing	40	4.4500	.74936

The results as shown in Table 4.9 indicate that vendor lock-in, loss of governance, cloud service termination, availability of services, intercepting data in transit and the risk of

enforcing contracts that span various jurisdictions have a mean score of 4.45 which implies that banks will face these risks to a large extent when adopting Cloud Computing. The risk of compliance had a mean score of 4.35 which also implies to a large extent banks will face this risk. However risks such as licensing, distributed denial of service, data transfer bottlenecks, resource exhaustion and loss of business reputation had mean scores lying between 2.65 and 3.23 which according to the scale imply they will be faced to a moderate extent when adopting Cloud Computing.

4.6 Mitigation Strategies

The fourth objective of the study was to determine the strategies a bank can use to mitigate the risks relating to Cloud Computing in the Kenyan Banking industry. The respondents were asked to rate the suitability of the listed mitigation strategies. A numerical score of 1=Strongly Disagree; 2=Slightly Disagree; 3=Undecided; 4=Slightly Agree; 5=Strongly Agree was coded and used to analyze the results as shown in Table 5.0.

Table 5.0 Mitigation Strategies

	N	Mean	Std. Deviation
To which degree do you agree Reviewing of vendor's internal audit process as the suitable strategy for your bank in mitigating risks relating to Cloud Adoption	40	4.2500	.83972

To which degree do you agree Determining of the frequency a vendor is audited by external agencies as the suitable strategy for your bank in mitigating risks relating to Cloud Adoption	40	4.2500	.77625
To which degree do you agree Establishing of the level of control surrounding the content and applications on the cloud as the suitable strategy for your bank in mitigating risks relating to Cloud Adoption	40	4.3500	.83359
To which degree do you agree Carry out a feasibility study to find out if the vendor is addressing the specific needs of the bank as the suitable strategy for your bank in mitigating risks relating to Cloud Adoption	40	4.1500	.94868
To which degree do you agree Drafting a agreements that identify and define a customers need [Quality of Service] in simple terms as the suitable strategy for your bank in mitigating risks relating to Cloud Adoption	40	4.2500	.86972
To which degree do you agree Drafting agreements that reduce areas of conflict and encourage dialogue in the event of a dispute as the suitable strategy for your bank in mitigating risks relating to Cloud Adoption	40	4.5000	.64051
To which degree do you agree Having a standard cloud Application Programming Interface [API] for ease of mitigating data between service providers as the suitable strategy for your bank in mitigating risks relating to Cloud	40	4.1750	.90263

Adoption			
To which degree do you agree Engaging vendors who are proactive and constantly train their customers on how to utilize Cloud Services as a suitable strategy for your bank in mitigating risk relating to Cloud Adoption	40	3.8500	.83359
To which degree do you agree Have cloud intermediaries/resellers put a performance bound or a financial ESCROW as the suitable strategy for your bank in mitigating risks relating to Cloud Adoption	40	3.8500	.80224

Table 5.0 shows that the mean scores for the mitigation strategies under investigation are between 3.85 and 4.5 which according to the scale imply that most of the respondents agree with the strategies was ways to mitigate the risks of Cloud Computing.

CHAPTER FIVE: SUMMARY CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This chapter summarizes and makes conclusions on the findings of the study in relation to the objectives as indicated in Chapter One. This chapter further discusses the limitations of the study and makes recommendations for areas for further research.

5.2 Summary of the Findings

5.2.1 Demographic Information

The respondents were ICT managers or their equivalents or ICT security practitioners in the banks. The study established that 57.5% of the respondents were male. 60% of the respondents were between the age of 36 and 40. 62% of the respondents had attained degree level of education and a further 8% had gone further and attained post graduate level. 52% of the respondents were ICT managers. 80% of the respondents were from banks whose total asset value lies between 10 and 40 billion and 60% of the banks the respondents came from were locally owned institutions.

5.2.2 Extent of Cloud Computing Adoption

The first objective of the study was to establish the extent Cloud Computing has been adopted by banks in Kenya. Descriptive statistics were used to analyse the collected data, the results were presented in tables. The findings indicate that most banks have not adopted Cloud Computing for their core areas while some of the banks have adopted Cloud Computing for applications such as Enterprise Resource Planning, Customer Relationship Management, Office Email and Mobile Banking.

5.2.3 Benefits of Cloud Computing

The second objective of the study was to determine the benefits of adopting Cloud Computing technology for banks in Kenya. Descriptive statistics were used to analyse the data collected. The study found out that Cloud Computing enables banks to save on costs while delivering services without compromising on security. The study findings showed Cloud Computing allows banks to convert high capital expenditures into operational costs that are more manageable. Using Cloud Computing, banks are able to reach their customers in new interactive ways as well as innovate in a faster more efficient way.

5.2.4 Cloud Computing Risks

The third objective of the study was to determine the risks banks face while adopting Cloud Computing. The study found out that risks like; vendor lock-in, loss of governance, data security and the enforcing legal contracts that span various jurisdictions ranked highly amongst the respondents and were a deterrent to adopting Cloud

Computing. In addition statutory requirements hinder Kenyan banks from adopting Cloud Computing due to compliance challenges with the industries regulator. Although once the issue of security and statutory requirements most banks are willing to venture into Cloud Computing.

5.2.5 Mitigation Strategies

The fourth objective of the study was to determine the mitigation strategies that banks can employ when adopting Cloud Computing. The study found that the mitigation strategies that can be employed by banks in Kenya include placing adequate audit controls and well defined policies and procedures that enforce IT governance, as well as defining standard protocols for cloud services that allow for data migration between service providers.

5.3 Conclusion

The findings established that majority of the banks in Kenya have not deployed their applications on the Cloud Computing and those who have, have done so using a cautionary approach of deploying non-core applications such as office email and mobile banking which the bank has no control over since the service provider has deployed their application on the Cloud.

The study established that the banks are well aware of all the benefits Cloud Computing offers such as reducing upfront IT costs, reducing IT maintenance costs, standardizing business processes that allows business to operate efficiently, provide new ways of

engaging customers, ensuring IT services are provided despite limited resources and reducing the total cost of ownership. Despite these benefits, Cloud Computing has risks that banks are aware of that were categorized into security and policies and procedures that need to be addressed before banks are able to adopt Cloud Computing technology.

The study established the following mitigation strategies that can be used to safe guard against the risks faced when adopting Cloud Computing: reviewing the internal audit process of Cloud vendors, determining the frequency and the willingness of Cloud vendors to be audited for compliance, establishing the level of control surrounding data and applications on the Cloud, defining agreements that reduce conflicts when an issue arises as well as identify and define a customer's specific needs, having standard cloud intermediaries/resellers put a performance bond on escrow in the event the vendor fails to maintain the desired service levels they have something to lose also.

5.4 Recommendations

The study has shown that the benefits of scalability, reliability, security, ease of deployment and ease of management can both be a friend and a foe from a security standpoint due to risks like data privacy, availability, performance and ownership but service providers are working to overcome these pitfalls. It is recommended for banks that want to experiment with Cloud Computing to evaluate the current risks and mitigation strategies for safe and successful Cloud Computing implementations. According to the Cloud Security Alliance (2009), Cloud Computing requires good governance, risk management and common sense on the part of organizations.

5.5 Limitations of the Study

Cloud Computing is a broad subject and the study was limited to its overall benefits and not benefits specific to each deployment model. The limitation of resources made it difficult to obtain responses from different banks. The study targeted ICT managers working in banks or their equivalents and did not interview ICT managers in other organizations as well as vendors of Cloud services who could have given more insights into Cloud Computing.

Another significant limitation of the study was the fact that Cloud Computing is relatively new and sufficient literature on the topic is not available some of the respondents had to inquire from peers and colleagues to complete the questionnaire.

5.6 Recommendations for Further Study

Based on the study findings, the following study areas may provide additional insights for further research:

- 1) Critical success factors for Cloud Computing implementations
- 2) Most suitable Cloud Computing model for banks to deploy on

Higher level studies can also be designed in such a way that they investigate cause/effect relationships using advanced statistical data analysis techniques.

REFERENCES

Abadi, D. (2009). Data management in the cloud: Limitations and opportunities. Bulletin of the IEEE Computer Society Technical Committee on Data Engineering.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., et al. (2009). Above the Clouds: A Berkeley view of cloud computing.

Awuondo, I. (2008). Commercial Application of ICT in the Banking Sector.

Betcher, J., T. (2010). Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners.

Buyya, R. , Yeo, C. , & Venugopal, S. (2008). Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities.

Central Bank of Kenya, (2011). Banking Act of Kenya Cap 488.

Central Bank of Kenya, (2012). www.centbank.go.ke/financialsystem/banks/Introduction.aspx, accessed on 5th July 2012.

Christiansen, C., Hudson, S., Kolodgy, C., & Pinal, G. (2010). Identity and Access Management for Approaching Clouds.

Cloud Security Alliance. (2009). Security guidance for critical areas of focus in cloud computing.

Cutler, N.E., & Gregg, D.,W., (1991). The Human Wealth Span and Financial Well-Being in Older Age.

Douglis, F. (2009). Staring at clouds. *Internet Computing, IEEE*, 13(3), 4-6.

ENISA. (2009). Cloud computing: benefits, risks and recommendations for information security.

Erdogmus, H. (2009). Cloud Computing: Does nirvana hide behind the nebula?

Feuerlicht, G., & Govardhan, S. (2009). SOA: Trends and Directions. *Systemes Integration*, 1-7.

Finnie, S. (2008, October 6). Peering behind the cloud. *Computerworld*, p. 22.

Furht, B., & Escalante, A. (2010). *Handbook of cloud computing*.

Gartner. (2011). Cloud Computing can Drive 'Creative Destruction' in the Banking Industry.

Gatewood, B. (2009). Clouds on the information horizon: How to avoid the storm. *Information Management (15352897)*, 43(4), 32-36.

Gay, L.R. (1981). *Educational Research: Competencies for Analysis and Application*.

Gewald, H., & Dibbern, J. (2009). Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. *Information & Management*.

Hall, H., B., & Khan, B. (2002). *Adoption of New Technology*

Harris, G., J., & Alter, E., A (2010). *Cloud Rise: Rewards and Risks at the Dawn of Cloud Computing*.

Hofmann, P., Jordan, J., & Brynjolfsson, E. (2010). *Cloud Computing and Electricity: Beyond the Utility Model*. *Communications of the ACM*.

IBM, (2010). *Cloud Computing Insights from 110 Implementation Projects*.

ISACA. (2009a). Cloud Computing: Business benefits with security, governance and assurance perspectives.

Jericho Forum. (2009). Cloud cube model: Selecting cloud formations for secure collaboration.

Kandukuri, B., Paturi, V., & Rakshit, A. (2009). Cloud security issues.

Kaufman, L. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE*, 7(4).

KPMG. (2009). Technology Paradigms for the Banking Industry

Leavitt, N. (2009). Is cloud computing really ready for prime time?

Mell, P., & Grance, T. (2009). The NIST Definition of Cloud Computing.

Microsoft. (2010). Software, Platforms and Infrastructure Solutions, The new World of Cloud Computing.

Mugenda, O., & Mugenda, G., (1999). Research Methods Quantitative and Qualitative Approaches.

Porter, M.E. and Millar, V.E. "How Information Gives You Competitive Advantage,"
Harvard Business Review (63:4), July-August 1985, pp. 149-160.

Price Water House Cooper, (2012).<http://www.pwc.com/ke/en/industries/banking.jhtml>,
accessed on 23rd October 2012.

Qamar, S., Lal, N., & Singh, M. (2010). Internet Ware Cloud Computing: Challenges.

Radhakrishnan, A., Zu, X., & Grover, V. (2006). A process-oriented perspective on
differential business value creation by information technology: An empirical
investigation. Omega, The International Journal of Management Science , 1-21.

Rash, W. (2009). Is cloud computing secure? Prove it. eWeek, 26(16), 8-10.

Rai, S., & Chukwuma, P. (2009). Security in a cloud. Internal Auditor, 66(4), 21-23.

Ryan, V. (2008). A place in the cloud. CFO, 24(8), 31-35.

Smith, J. (2009). Fighting physics: A tough battle. Communications of the ACM, 52(7),
60-65.

Sriram, S. (2011). Cloud Computing in Banking.

Stanoevska-Slabeva, K., & Wozniak, T. (2010). Cloud Basics - An Introduction to Cloud Computing (2 ed.).

Vaquero, L. M. (2009). A Break in the Clouds: Towards a Cloud Definition.

Van Elst, M. (2010). Advanced IT outsourcing by using the Cloud Computing model.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & StèoBer, J. (2009). Cloud computing - A classification, business models, and research directions. *Business & Information Systems Engineering*, 1(5), 391-399.

Willcocks, L., Venters, W., & Whitley, A., E. (2011). Meeting the Challenges of Cloud Computing.


Wooley, S. P. (2011). Identifying Cloud Computing Security Risks.

Youseff, L., Butrico, M., & Da Silva, D. (2008.) Toward a unified ontology of cloud computing. *Grid Computing Environments Workshop*, 2008.

APPENDICES

Appendix 1: Letter of Introduction

180 C 15


UNIVERSITY OF NAIROBI
SCHOOL OF BUSINESS
MBA PROGRAMME

Telephone: 020-2059162
Telegrams: "Varsity", Nairobi
Telex: 22095 Varsity

P.O. Box 30197
Nairobi, Kenya

DATE: 25/9/2012

TO WHOM IT MAY CONCERN


The bearer of this letter: PASHID JAMES MUNGAE
Registration No. D61/75722/2009


is a bona fide continuing student in the Master of Business Administration (MBA) degree program in this University.

He/she is required to submit as part of his/her coursework assessment a research project report on a management problem. We would like the students to do their projects on real problems affecting firms in Kenya. We would, therefore, appreciate your assistance to enable him/her collect data in your organization.

The results of the report will be used solely for academic purposes and a copy of the same will be availed to the interviewed organizations on request.

Thank you.


IMMACULATE OMANO
MBA ADMINISTRATOR
MBA OFFICE, AMBANK HOUSE


UNIVERSITY OF NAIROBI
SCHOOL OF BUSINESS
25 SEP 2012
MBA OFFICE
P.O. Box 30197 - 00100, NAIROBI

Appendix 2: Questionnaire

Section A: Individual and Organizational Bio Data

1) What is your gender?

Male []

Female []

2) What is your age bracket?

Below 25 years []

26 – 30 years []

31 – 35 years []

36 – 40 years []

41 - 45years []

46 – 50 years []

Above 50 years []

3) What is your highest level of education?

O Level []

A Level []

Diploma []

Degree Level [] Post Graduate Level []

Others: _____

4) What is your job title?

Banking Operations

IT Security Practitioner

Business Analyst

ICT Manager

Others _____

5) What is the size of the bank in terms of value of total assets?

Below Ksh 10 Billion

Between Ksh 10 Billion and Ksh 40 Billion

Above Ksh 40 Billion

6) In which category does your bank fall in?

Foreign Owned Not Locally Incorporated

Foreign Owned but Locally Incorporated

Foreign Owned but Locally Incorporated with Partial Local Ownership

Institutions with Government Participation

Locally Owned Institution

Section B: Extent of Cloud Computing Adoption

7) Please indicate on the scale given by ticking [√] in the appropriate boxes the extent to which Cloud Computing has been adopted for the following services in your bank.

- 1) No Extent 2) Little Extent 3) Moderate Extent 4) Large Extent
 5) Very Large Extent

SERVICE	1	2	3	4	5
Point of Sale (POS)					
ATM					
Mobile Banking					
Internet Banking					
Customer Relationship Management					
Enterprise Resource Planning					
Core Banking [Deposits and Credit Facilities)					
Trade-Finance					
Treasury					
Office Email					
Others, specify and rate accordingly					

Section C: Benefits of Cloud Computing

8) Please rate on the scale given by ticking [√] in the appropriate boxes the extent to which you agree as to the benefits that your Bank could realize on adopting Cloud Computing

- 1) No Extent 2) Little Extent 3) Moderate Extent 4) Large Extent
 5) Very Large Extent

BENEFIT	1	2	3	4	5
Reduced up front IT Cost					
Reduced cost of maintaining IT infrastructure					
Improved communication and collaboration between individuals					
Standardized and efficient business processes					
Provision of new ways to engage and interact with customers					
Assured IT services with limited resources					
Faster Product/Service Development					
Rapid changing of business processes					
Improved analytical capabilities					
Enabled processes that are not otherwise cost-effective or feasible					
Facilitation of efficient data exchange with external organizations					
Establishment of uniform processes in different regions					
Development of products or services that were not feasible before					
Reduced energy consumption					
Others, specify and rate accordingly					

Section D: Cloud Computing Risks

10) Please indicate on the scale below by ticking [√] in the appropriate boxes the extent to which your bank faces each of the following risk in the adoption of Cloud Computing.

- 1) No Extent 2) Little Extent 3) Moderate Extent 4) Large Extent 5) Very Large Extent

CLOUD COMPUTING RISK	1	2	3	4	5
Vendor Lock-in					
Loss of Governance					
Compliance Challenges					
Loss of Business Reputation					
Cloud Service termination or failure					
Availability of Service					
Resource Exhaustion					
Intercepting data in transit					
Data transfer bottlenecks					
Distributed denial of service					
Subpoena and e-discovery					
Changes of jurisdiction					
Data privacy					

Licensing					
Others, specify and rate accordingly					

Section E: Mitigation Strategies

11) The following are strategies for mitigating risks relating to Cloud Computing. For each strategy indicate on the scale given by ticking [√] in the appropriate box the degree to which you agree as to the suitability of each strategy for your bank.

- 1) Strongly Disagree 2) Slightly Disagree 3) Undecided 4) Slightly Agree
 5) Strongly Agree

MITIGATION STRATEGY	1	2	3	4	5
Reviewing of a vendor's internal audit process					
Determining of the frequency a vendor is audited by external agencies.					
Determining if a vendor is willing to be audited for compliance					
Establishing of the level of control surrounding the content and applications on the cloud.					

Carry out a feasibility study to find out if the vendor is addressing the specific needs of the Bank					
Drafting agreements that identify and define a customers' needs [Quality of Service] in simple terms					
Drafting agreements that reduce areas of conflict and encourage dialogue in the event of a dispute					
Drafting agreements that eliminate un-realistic expectations					
Having a standard cloud Application Programming Interface [API] for ease of migrating data between service providers					
Engaging vendors who are proactive and constantly train their customers on how to utilise Cloud Services					
Others, specify and rate accordingly					

Appendix 3: List of Commercial Banks in Kenya

1. Bank of Africa (K) Ltd.
2. Bank of India.
3. Citibank N.A. Kenya.
4. Habib Bank A.G. Zurich.
5. Habib Bank Ltd.
6. Bank of Baroda (K) Ltd.
7. Barclays Bank of Kenya Ltd.
8. Diamond Trust Bank Kenya Ltd.
9. K-Rep Bank Ltd.
10. Standard Chartered Bank (K) Ltd.
11. Ecobank Ltd.
12. Gulf Africa Bank (K) Ltd.
13. First Community Bank.
14. UBA Kenya Bank Limited.
15. Consolidated Bank of Kenya Ltd.
16. Development Bank of Kenya Ltd.
17. Housing Finance Ltd.
18. Kenya Commercial Bank Ltd.
19. National Bank of Kenya Ltd.
20. CFC Stanbic Bank Ltd.
21. African Banking Corporation Ltd.

22. Jamii Bora Bank Ltd.
23. Commercial Bank of Africa Ltd.
24. Co-operative Bank of Kenya Ltd.
25. Credit Bank Ltd.
26. Charterhouse Bank Ltd.
27. Chase Bank (K) Ltd.
28. Dubai Bank Kenya Ltd.
29. Equatorial Commercial Bank Ltd.
30. Equity Bank Ltd.
31. Family Bank Ltd.
32. Fidelity Commercial Bank Ltd.
33. Fina Bank Ltd.
34. Giro Commercial Bank Ltd.
35. Guardian Bank Ltd.
36. Imperial Bank Ltd.
37. Investment & Mortgages Bank Ltd.
38. Middle East Bank (K) Ltd.
39. NIC Bank Ltd.
40. Oriental Commercial Bank Ltd.
41. Paramount Universal Bank Ltd.
42. Prime Bank Ltd.
43. Trans-National Bank Ltd.
44. Victoria Commercial Bank Ltd.