"A SURVEY OF ICT AUDIT IN COMMERCIAL BANKS IN KENYA"

BY

NZUKI, CHARLES KYALO

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

OCTOBER, 2006

DECLARATION

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

Signed CN Date 8th November, 2006

NZUKI CHARLES KYALO

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

Signed Lelei Date 17th November 200

JOEL K.LELEI

Lecturer, Department of Management Science

School of Business

University of Nairobi

DEDICATION:

I dedicate this project to my wife Naomi and our beloved sons Kenneth and Kevin for affording me time to study for MBA at the University of Nairobi

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

Firstly, my acknowledgement goes to my supervisor Mr. Joel K. Lelei for his professional guidance and support provided to me to complete this project. Secondly, I acknowledge my immediate and extended family as well as the many honest friends who cheered me on when I wanted to give up. Thirdly, to all my MBA lecturers and student colleagues who added value not only to my studies but life in general, many thanks and God bless them all.

ABSTRACT

Given the increasing reliance on Information Communication Technology (ICT) systems for managing business processes, as well as driving business strategy, ICT auditing has become a requirement of international standards on auditing. In Kenya, the Central Bank stipulates that commercial banks undertake ICT audits as a measure of disaster recovery and business continuity plans, among other key ICT controls. With increased use of computer based-information systems, commercial banks have become more exposed to risks that could result into gross financial losses. This has resulted to increased demand for assurance to the management and other stakeholders that the business's ICT systems are operating as intended.

In Kenya, commercial banks have implemented different levels of ICT auditing. The extent of ICT auditing on the specific aspects and challenges faced in ICT auditing was a major concern and needed to be known. It was in view of this that this study was conducted with the following objectives: to determine the extent of ICT auditing in banks in Kenya and to establish the challenges faced in effort to successful ICT auditing in banks in Kenya. The study was an exploratory survey targeting all commercial banks with operations in Nairobi. The design was appropriate considering that not much was known to make it possible to do a more advanced research. Data collection was done through a questionnaire. Of the 46 commercial banks targeted for the study, there were 38 fully completed questionnaires which represented an 82.6 % response. Data collected from the respondents was analyzed using various statistical tools and findings were found adequate to make inferences and generalization of the state of ICT auditing in commercial banks in Kenya.

Findings of the study indicated that most of the commercial banks in Kenya had awareness about and conducted ICT audits regularly. ICT auditing was being undertaken by either the internal audit departments or by external auditors. Most international and foreign owned banks exhibited thorough and in-depth ICT audit practices mainly being done by their company group audit teams with high level of specialization and sophistication as compared to the locally owned and the privately owned banks. All banks interviewed showed evidence of ICT auditing processes that focused on confidentiality, integrity and availability aspects of their ICT based systems. There was consensus among the respondents on frequency of ICT audits and on ICT audits around aspects relating to the overall business continuity planning.

The study found that ICT auditing among Kenya's commercial banks faced numerous challenges. Poor assessment of threats and vulnerabilities was found to be the most challenging factor as well as the lack of awareness about ICT auditing by senior managers. Other major challenges were related to the complexity of ICT infrastructure and poorly defined compliance framework for Kenya. The concept of ICT auditing was hence found to be a newly emerging phenomenon and hence existing gaps and lack of standard ICT audit framework/guidelines was found to be a challenge especially among the smaller banks. In addition, the complexity of the ICT auditing exercise coupled to ICT being a highly technical field, ICT auditors required specialized skills which in most cases were not readily available among the conventional audit teams.

In view of the above and in summary, this study gave a general view of the state of ICT auditing in commercial banks in Kenya and outlined the extent of ICT auditing as well as the major challenges that banks face in their effort to successful ICT auditing. The greatest beneficiary of this study was the society which would enjoy greater confidence in information systems if commercial banks undertook successful ICT audits. There were a few limitations encountered while undertaking this study. Firstly, some respondents and mainly from the privately owned banks were reluctant to disclose information relating to the topic and as a result the number of completed questionnaires was reduced. Secondly, the target respondents were IT managers and some could not provide information regarding to the size in terms of staffing and number of accounts which were necessary to determine the size of the bank. Further research should be undertaken on the topic through a case study on ICT auditing specific to any of the main commercial banks: Standard Chartered, Barclays Bank or Kenya Commercial bank in order to get an in-depth understanding of the topic.

LIST OF TABLES

Page

LIST OF FIGURES

LIST OF ABBREVIATIONS

ICT	Information Communication Technology
DES	Data Encryption Standard
EDP	Electronic Data Processing
EDPAA	Electronic Data Processing Auditors Association
ISACA	Information Systems Audit and Control Association
AIS	Accounting Information Systems
CAATTs	Computer Aided Audit Tools and Techniques
IIA	Institute of Internal Auditors
DRP	Disaster Recovery Planning
NBFI	Non-bank Financial Institution
FIRST	Financial Sector Reform and Strengthening
NBK	National Bank of Kenya
KCB	Kenya Commercial Bank
NSE	Nairobi Stock Exchange
FSAP	Financial Sector Assessment Program
ATM	Automated Teller Machine
MICR	Magnetic Ink Character Recognition
EFTPOS	Electronic Funds Transfer at Point of Sale
EFT	Electronic Funds Transfer

CHAPTER ONE:

INTRODUCTION

1.1 Role of ICT in Organization

The use of Information and Communication Technology (ICT) has become increasingly significant in recent years in all sectors of global economies whether in the public, private sectors as well as in non-governmental organizations. ICT is now an integral part of all processes that enable businesses and governments to accomplish their missions and objectives (Vowler, 2003). ICT has revolutionized the nature and scope of worldwide communications, changed business processes, and erased the traditional boundaries of the organization — internally between departments and externally with customers and service beneficiaries (Harvard business Review: September – October, 1995). This demonstrates the power of ICT as both a driver and enabler of management processes and strategies.

Businesses are heavily relying upon ICT to create competitive advantage thereby taking a new urgency to the business. Today, ICT plays a role in most aspects of a company's business and operations, from development of new products to the support of sales and services provision, from providing market intelligence to supplying tools for decision analysis (Harvard business Review: September – October, 1995). ICT application has widened in scope, extending beyond businesses to public sector for better services delivery

In January, 2006, the Kenyan government through the ministry of Information and Communications issued the National Information & Communication Technology (ICT) policy (Ministry of Information & Communications). Through the ICT policy and the closely related e-Government strategy, the government has a mission "to use information and communication Technology to improve the livelihoods of the people of Kenya and optimize its contribution to the development of the economy by ensuring the availability of efficient, reliable and affordable info-communication services throughout the country" (Kenya's ICT policy, 2006). This is an indication of how ICT has become critical in all areas of day-to-day business and provision of services in sectors of the Kenyan economy.

Business managements and government entities have objectives and high expectation when deploying ICT systems. Reasons for implementing ICT within the private and public organizations include the desire to obtain value through reduced costs, greater effectiveness, enhanced efficiency and increased service delivery. In view of the increased demand for reliability on ICT systems there is need for assurance on the status of firm's ICT. Generally stakeholders are concerned about confidentiality, integrity, availability, reliability and compliance with legal and regulatory requirements (Hickman, 2000). Thus ICT audit is inevitable.

A key aspect of ICT auditing is to provide assurance about the confidentiality, integrity and availability of an organization's information. In banking, information is critical for the business to engage in commercial activities. Loss of one or more of these attributes, can threaten the continued existence of even the largest corporate entities.

ICT audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allow organizational goals to be achieved effectively and uses resources efficiently. An effective information system leads the organization to achieve its objectives while an efficient information system uses minimum resources in achieving the required objectives (Chaplan, 1998). ICT audit is very critical in banks in view of the heavy reliance on ICT and the security of financial information they handle.

1.2 Overview of the Banking Sector in Kenya

Kenya's financial system is among the more developed in Sub-Saharan Africa, with a large banking sector. The banking sector is comprised of one non-bank financial institution (NBFIs), 2 mortgage financial companies, 2 building societies, 15 microfinance institutions, 3800 savings and credit cooperatives, 89 foreign exchange bureaus and 42 commercial banks, with the six largest accounting for about two-thirds of all assets, loans and deposits of the banking system (The Financial Sector Reform and Strengthening (FIRST) Initiative, 2006).
Of the four main banks, two—Barclays and Standard Chartered— are subsidiaries of foreign banks and are by far the most profitable, while two —Kenya Commercial Bank (KCB) and the National Bank of Kenya (NBK)—are mainly state owned.

The banks, NBFIs, microfinance institutions and building societies are supervised by the Central Bank of Kenya while Savings and Credit Cooperatives are regulated by the Commissioner of Cooperatives. No one person can own more than 25% of a commercial bank and the government does not fully own any commercial banks however it does maintain ownership shares in four major commercial banks. Recent developments include the creation of a formal deposit insurance scheme, the Deposit Protection Fund. Also, in June 2005, the CBK finalized plans for electronic money transfers between banks—Real Time Gross Settlement—allowing for the instantaneous movement of funds (The Financial Sector Reform and Strengthening (FIRST) Initiative, 2006).

The Nairobi Stock Exchange (NSE) is Kenya's only stock exchange and the center of its capital markets sector. The NSE listed 48 firms in early 2004, including many financial companies and industrial firms. The supervision and regulation of the capital markets sector is the responsibility of the Capital Markets Authority. In partnership with the IMF, the World Bank completed a Financial Sector Assessment Program (FSAP) in May 2005 which identified potential vulnerabilities and developmental needs for the sector as well as the risks to macroeconomic stability from weaknesses and shortcomings in the financial sector.

The clearing and payment between banks has been efficiently processed through the Automated Clearing House using Magnetic Ink Character Recognition based technology cheques and Electronic Funds Transfer systems. Cash is the most common form of payment media used however it has the major disadvantage of being insecure, bulky and costly to produce (Central Bank of Kenya, 2004).

1.3 ICT in Banks

Banks have made extensive use of ICT in their day to day activities. ICT is used in Magnetic Ink Character Recognition (MICR) systems where characters are written in a special magnetic ink, and have the advantage that they can be read by a reader connected to a computer, Bankers' Automated Clearing Services (BACS) have deployed ICT to carry out most financial transactions between banks including clearing cheques, paying in salaries and payment of standing orders or direct debits. ICT is used widely used in Electronic Funds Transfer at Point of Sale (EFTPOS), Electronic Funds Transfer (EFT) systems and for Smart

Cards operations. All these allow funds to be transferred from the customer's account to the retailer's account.

Automated Teller Machines (ATM) widely deployed by banks extensively use ICT. ATMs are connected to the bank via telecommunication lines and pass details of each transaction to a transaction file to be processed by a central computer. An ATM allows customers to make withdrawals, get account statements as well as make deposits. For the customer, the ATM is more anonymous, provides a 24-hour a day service, seven days a week hence proving a lot of flexibility and fewer queues since the transactions are quicker. For the bank, ATM system frees up staff from performing routine transactions so that more profitable work can be done, reduces the number of staff and provides a continuous service outside normal hours. ICT is the widely used in Internet Banking.

As the backbone of e-commerce. ICT has been described as the greatest opportunity and greatest threat facing banks (Rosenoer, Armstrong, and Gates, 1999). Not only has ICT changed the way banks conduct their business, but it has also increased the risk and the level of controls needed. The increased risk resulted from (1) the organization's inability to continue business if systems are not functioning properly, and (2) the use of ICT to operate globally and interconnect with outside entities (Vowler, 2003). Any failure on the backbone of e-commerce is catastrophic to both the business and the clients and thus the need for constant checks on ICT systems.

The level of use and reliance on ICT in banking is alarming such that in critical systems failure entire operations come to a halt (Advanced Information Technology). In some organizations the entire data has been computerized and all information is available only in digital form. Thus ICT controls are of great value in any computerized system and it is important task to see that not only do adequate controls exist but that they also work effectively to ensure results and achieve objectives. ICT auditing evaluates the adequacy of internal controls in computer systems to mitigate the risk of loss due to errors, fraud and other acts and disasters or incidents that cause the system to be unavailable (Le Grand, 2001).

1.4 Problem Statement

Benefits of ICT together with customer expectations have made banks to integrate ICT into their everyday activities. Thus banks have tended to rely heavily upon ICT which has placed it amongst the most critical components that determine the survival of the business in the market place. ICT failures would then be catastrophic and hence a major concern. In view of this, ICT auditing has become very critical.

ICT audit evaluates the effectiveness and efficiency of ICT controls and the closely related ICT security plans in information systems together with their underlying operation procedures to ensure they operate as intended (Doyle, 1997). An effective ICT Audit is essential to put the company in a position to understand the complete impact that the Information and Communication Technology environment has on its business performance and allow it detect and mitigate potential problem areas early. ICT audits may be limited or extensive with diverse range of aspects and may be faced with various challenges depending on situation. ICT auditing approaches will thus tend to vary from firm to firm based on level of usage of ICT, physical and human factors, policies and level of integration with third party services.

In Kenya, ICT auditing is a newly emerging phenomenon. Thus not much research has been done on the subject. Studies have been conducted to evaluate the level of usage of ICT in Kenyan firms (Nyambane, 1996), a survey of the causes of IS failure among microfinance institutions in Kenya was conducted by Ndulu, 2004 aimed at identifying the state of ICT among microfinance institutions in Kenya. Ndulu's findings exposed factors underlying the failure of Information Systems among the microfinance institutions as financial constraints, unreliable telecommunications, poor training of users as well as defective system development process among others (Ndulu, 2004). In view of these findings, a study on ICT auditing as a solution to alleviating the problems identified is necessary. Mbote, (2003) looked at the influence of ICT on marketing with special focus to the commercial banks. Mbote's findings indicated that ICT has greatly influenced the marketing strategies and approaches and hence emphasized its criticality to commercial banks.

The level of deployment of ICT among Kenyan firms is varied (Nyambane, 1996). In view of this, there is an expected variation on the extent of ICT auditing among the various businesses, industry sectors as well as variation on the challenges faced by different firms in effort to effective ICT audit implementation. Approaches to ICT auditing would likewise have to vary from firm to firm. How these variations are in commercial banks is the subject of this research. Thus this study addresses three questions: what is the extent of ICT auditing conducted in commercial banks, what aspects are covered by the audits and what challenges do the banks face in effort to successful ICT auditing?.

1.5 Objectives of the Study

This research has two specific objectives

1. To determine the extent of ICT audit in banks in Kenya.
2. To establish the challenges of ICT audit in banks in Kenya

1.6 Importance of the Study

Findings from this study will be of interest to the following:-

Banking Industry in Kenya

Banks in Kenya draw upon the findings of this study to gauge their performance as far as their ICT auditing is concerned.

Audit firms and Consultants

The study documented the extent, aspects of ICT auditing as well as the challenges faced in the effort to achieve successful auditing in the banking industry in Kenya. The extent to which ICT auditing was being undertaken identified gaps presenting potential business target by audit firms and consultants to expand on their market and clientele base. Challenges faced in ICT audit would make the auditors to be more prepared as they plan their audits in banks in Kenya.

Learning Institutions

Academics may use the findings of the study as a basis for further research in ICT auditing. The study is expected to stimulate more academic research on ICT auditing topics. A comparative study may be necessary to document the variations of ICT audit among different sectors in Kenya.

Professional Bodies

Professional bodies e.g. Computer Society of Kenya would be interested by the findings of this study as an advisory organ in provision of auditing guidelines and development of an ICT audit framework for Kenya. Understanding of the extent of ICT audit in the banks and the challenges faced would be useful so as to offer intelligent professional guidance relating to enhancement of ICT auditing.

Government of Kenya

The Central Bank of Kenya has a regulatory function over the banking industry in Kenya. To accomplish this task the bank issued the prudential guidelines for institutions licensed under the banking act. The Guideline issued under Section 33(4) of the Banking Act, stipulates the licensing and compliance requirements to be adhered to by institutions in order to maintain a stable and efficient banking and financial system. ICT Auditing among the financial institutions is one of the major concerns of the central bank as part of stabilizing and enhancing efficiency in the banking sector and hence the findings from this study would be of interest to the central bank.

Government agencies and institutional bodies like the ministry of Information and Communication would be interested in knowing the extent of ICT audit in the banking industry. This would be a useful input in making policy decisions relating to ICT in Kenya. Implementation of the ICT policy and the e-government strategy documents would require a functional e-commerce network as it involves transfer of assets and money. The required ICT compliance in the banking sector can only be verified through ICT auditing since most systems have integrated technology and hence the findings of the extent of the practice is useful.

CHAPTER TWO:

LITERATURE REVIEW

2.1 Auditing

Auditing, in general, is formally described as: "The independent examination of records and other information in order to form an opinion on the integrity of a system of controls and recommend control improvements to limit risks" (Warren, et al, 2001) The various types of audits are operational audits, financial and administration audits, compliance audits, ICT audits, special investigations audit (RMIT University). Computer auditing is a branch of general auditing concerned with governance (control) of information and communications technologies (computers). Computer auditors primarily study computer systems and networks from the point of view of examining the effectiveness of their technical and procedural controls to minimize risks.

ICT audit has also been defined as the process of collecting and evaluating evidence to determine whether computer systems have been designed to maintain data integrity, safeguard assets, allows organizational goals to be achieved effectively and uses resources efficiently. An effective information system leads the organization to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives (Computer Security Institute, 2003).

2.2 Confidentiality, Integrity and Availability

Confidentiality relates to the assurance that information is shared only among authorized persons or organizations. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc. The classification of the information should determine is confidentiality and hence the appropriate safeguards (Computer Security Institute, 2003). Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords, that uniquely identify data system users, and supporting control methods that limit each identified user's access to the data system's resources.

Integrity is concerned with the assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose is critical in banking. The term Integrity is used frequently when considering Information Security as it is represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon.

Availability of Information is critical to ensure that systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. ICT auditing is concerned with evaluation of information systems security, focusing on the three core goals of confidentiality, integrity and availability of information. Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate).

2.3 Impact of ICT Failure

Negative impacts of ICT failures in any industry include revenue loss, loss of share value, loss of interest on overnight balances, cost of interest on lost cash flow, delays in customer accounting, accounts receivable and billing/invoicing, loss of control over debtors, loss of revenue for service contracts from failure to provide service or meet service levels, loss of contract opportunities, penalties from failure to produce annual accounts or produce timely, tax payments. Other losses include cost of replacing equipment, cost of replacing software, cost of re-creation and recovery of lost data, loss of cash flow, loss of customers (lifetime value of each) and market share, loss of profits, fines and penalties for non-compliance and loss of credibility due to services being un-available (Computer Security Institute, 2003).

The banking industry is heavily reliant on both communication and ICT systems to provide services to the business world. Any failures to the IT infrastructure and lapses of controls cost businesses millions of dollars. In June 2003, a commercial bank in Kenya recorded a fraud where cash amounting to U.S Dollars 182,086 was withdrawn from six ATM points in Nairobi.

2.4 ICT Controls and Security

Today's paperless society, where any transaction is a click of a mouse away, is not without pitfalls as there are many emerging risks and threats being faced by businesses as a result of the extensive use of ICT based systems. IT-Web, 25 June 2004 released the second edition of the 'ICT Risk Check List', which identified more than 112 technology risks that threaten all banking businesses. "ICT risks and liabilities are starting to take a toll on businesses and managements are scrambling to protect their assets and reputations" (IT- web, June 2004).

"Some company directors are surprised to learn that ICT risks are not limited to viruses and hackers but extents to many aspects. It is all risks and more risks". Risks associated with use of technology by employees, external security risks, websites and e-commerce risks, willful and negligent actions by employees, unauthorized disclosure of trade secrets and private information by negligent employees, theft of computer equipment, software risks and general technology risks are just but a few examples of the increasing ICT risk profile (IT- web, June 2004).

As a consequence of the possible negative impact of using ICT systems, the confidentiality, integrity, availability and reliability of computerized data and of the systems that process, maintain and report these data are a major concern to the organization's management, staff and clients as well as the general public (Collis and Montgomery, 1995). It is in view of the diverse threats and vulnerabilities that banks are exposed to, that effective ICT controls, ICT security and ICT audits are critical to provide mitigation to the risks.

ICT controls in a computer information system are all the manual and programmed methods, policies and procedures that ensure the protection of the entity's assets, the accuracy and reliability of its records and the operational adherence to the management's standards. In an ICT environment, the control components found in manual systems must still exist however the use of computers affects the implementation of these components in many ways.

While manual and mechanical information processing systems use paper documents and other media that can be visually checked by information processing personnel, hence facilitating easier detection of errors and fraud, computer based systems on the other hand use machine sensible media such as magnetic tapes and accomplishes the processing within the circuitry of the system hence the ability to check visually the progress of the processing and the contents of the databases is significantly reduced (O'Brien 2001).

Varied controls are required to prevent computer failure or minimize its effects. Computers fail for several reasons ranging from power failure, electronic circuitry malfunctions. and mechanical malfunction of peripheral equipment, hidden programming errors and computer operator errors. Critical systems have to be fault tolerant for services continuity. ICT controls should support strategic, operations, reporting, and compliance and by ensuring that transactions are complete, accurate, authorized, and valid (Barker, 1998).

A functional IT security policy is a critical consideration for banks. This is where aspects of system confidentiality (restricting access to authorized users) as well as system availability (ongoing systems resources being available for organizational use) are addressed. Some of the ways in which computer online security is achieved are through encryption, Data Encryption Standard (DES), digital/electronic signatures and biometrics (Friedlob, Plewa, Schleifer, and Schou, 1997). There is increasingly high regulatory demand for organizations to protect consumer data. At the same time, organizational Web sites and intranets are under attack from hackers and others (Computer Security Institute, 2003).

Potential ICT security tools include multilevel access controls, smart cards, firewalls and their continuous monitoring, intrusion detection software, encryption, tracking the frequency of confidential inquiries, filtering, virtual private networks, and biometrics. Because many organizations operate as extended enterprises today, they must ensure the security of systems belonging to business partners and suppliers that have access to their systems (Barker, 1998).

2.5 ICT and Auditing

Use of computer facilities has brought about radically different ways of processing. recording and controlling information and has combined many previously separated functions. The potential for material systems error has thereby been greatly increased causing great costs to the organization. The highly repetitive nature of many computer applications means that small errors may lead to large losses. This makes it imperative for the auditor to test the invisible processes and to identify the vulnerabilities in a computer system as through errors and irregularities, the costs involved can be enormous.

It is believed that the first use of a computerized accounting system was at General Electric in 1954. During the time period of 1954 to the mid-1960s, the auditing profession was still auditing around the computer. At this time only mainframes were used and few people had the skills and abilities to program computers. This began to change in the mid-1960s with the introduction of new, smaller and less expensive machines (Auditing standards and guidelines, 1998).

Around 1960, EDP auditors formed the Electronic Data Processing Auditors Association (EDPAA). The goal of the association was to produce guidelines, procedures and standards for EDP audits. In 1977, the first edition of Control Objectives was published. This publication is now known as Control Objectives for Information and related Technology (CobiT). In 1994, EDPAA changed its name to Information Systems Audit and Control Association (ISACA). The period from the late 1960s through today has seen rapid changes in technology from the microcomputer and networking to the internet and with these changes came some major events that have altered the traditional auditing methodologies.

O'Brien, (2001) argues that there are three basic approaches for auditing information systems. These are auditing around the computer, auditing with the computer and auditing through the computer.

Auditing around the computer

Auditing around the computer involves verifying the accuracy and propriety of computer input and output without evaluating the computer programs used to process the data. It is a simpler and easier method that does not require auditors with programming experience (O'Brien, 2001). However this auditing does not trace a transaction through all of its stages of processing and does not test the accuracy and integrity of computer programs and hence recommended as a supplement to other auditing methods.

Auditing through the computer

Auditing through the computer involves an IS auditor following an audit trail as it proceeds within the internal computer operations phase of automated data processing. Through the computer auditing, attempts are made to verify the processing controls involved in the Accounting Information Systems (AIS) programs. This technique is used when auditing complex computer-based systems, especially on-line systems. The process includes test data approach, integrated test facility, and embedded audit modules or standardized from audit software developers. Test data technique uses a set of hypothetical data to audit the programmed checks in both transaction and non-transaction processing programs.

An audit trail is defined as the presence of documentation that allows a transaction to be traced through all stages of its information processing. The audit trail of manual information systems was quite visible and easy to trace, however this has changed with computer based information systems (O'Brien, 2001).

Auditing with the computer

Auditing with the computer uses Computer Aided Audit Tools and Techniques (CAATs). Increasing demands for assurances of computer systems, information security, controls over the privacy of data, and quality assurance practices makes it necessary to use CAATs. Auditors use a variety of Computer Assisted Audit Tools and Techniques, or CAATS (also known as CAATTs), which are computerized tools or techniques that increase the efficiency and effectiveness of the audit. CAATs include a wide variety of PC software tools that support a flexible, interactive, approach to verify data accuracy, completeness, integrity, reasonableness, and/or timeliness (Hickman, 2000).

2.6 ICT Audit Objectives

The objective of undertaking an IT audit is to evaluate a firm's computerized information system in order to ascertain whether the systems produces timely, accurate and reliable information outputs, as well as ensuring confidentiality, integrity, availability and reliability of data and adherence to relevant legal and regulatory requirements (Parker, 2001). The objectives of undertaking an ICT audit as a component of a financial audit statement include to understanding how well management capitalizes on the use of information technology to improve its important business processes.

ICT auditing helps the management to understand the pervasive effect of information technology on the client's important business processes, including the development of the financial statements and the business risk related to these processes. An ICT audit helps the management to conclude on the effectiveness of controls over the information technology processes that have a direct and important impact on the processing of financial information. Where ICT audit is involved in the performance audit, the objectives of the audit include providing assurance that all aspects of the ICT systems, including necessary controls are effectively enforced.

In addition, ICT audits provide assurance of compliance with all applicable laws because failure to comply and/or protect data exposes the organization to potential lawsuits, financial losses, and loss of reputation (Weber, 1999). ICT audit reviews the compliance with policies, plans, procedures, laws, and regulations. In this case the audit function is responsible for determining whether the systems are adequate and effective and whether the activities audited are complying with the appropriate requirements.

ICT audit critically reviews the ICT/network system security controls including reviewing information security controls during the testing phase of systems development, or on operational systems and networks (technical, physical and/or procedural controls; preventive, detective and/or corrective controls). The audit process conducts post-incident reviews to discover the root cause/s of information security incidents, reviews the ICT disaster contingency planning including the ICT elements of business continuity planning (Institute of Internal Auditors (IIA), 2000).

In addition ICT audits related to the economical and efficient use of resources should identify such conditions as under-utilized facilities, nonproductive work, procedures that are not cost justified and overstaffing or understaffing. Management is responsible for establishing operating or program objectives and goals, developing and implementing control procedures, and accomplishing desired operating or program results. The audit function should ascertain whether such objectives and goals conform to those of the organization (Institute of Internal Auditors (IIA), 2000).

2.7 Elements of an ICT Audit

An information system is not just a computer. Today's information systems are complex and have many components that piece together to make a business solution (Anderson, 2003). Assurances about an information system can be obtained only if all the components are evaluated and secured. The proverbial weakest link is the total strength of the chain holds in the case of ICT audit evaluation. The major elements of Information Systems audit can be broadly classified under the following categories (Computer Security Institute, 2003).

Physical and environmental review includes an assessment of the physical security, power supply, air conditioning, humidity control and other environmental factors while ICT installation audits do check the computer building, suite, room including aspects such as physical security (walls, CCTV, locks, guards, barbed wire, visitor procedures), environmental controls (fire and flood protection, power supply, air conditioning), computer and network operations processes and management systems, and the ICT equipment.

System administration aspect of the audit reviews the security of the operating systems, database management systems, all system administration procedures and compliance. Operational computer system/network audits review the controls within and surrounding operational computer systems and networks, at various levels including network, operating system, logical/procedural controls, preventive/detective/corrective controls, crypto, logging.

Application software audits review the business applications or an enterprise resource planning system that actually runs the business. Review of such application software includes access control and authorizations, validations, error and exception handling, business process flows within the application software and complementary manual controls and procedures. Applications development systems audits typically cover either or both of two aspects of project/programme management controls and the specification, development, testing, implementation and operation of technical and procedural controls (Computer Security Institute, 2003).

Network security review checks the internal and external connections to the system, perimeter security, router access control lists, port scanning and intrusion detection aimed at verifying that the network environment is properly secured while ICT business continuity aspect of the audit reviews the existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan. Disaster contingency/business continuity planning/disaster recovery audits evaluate the arrangements of restoring some semblance of normality after a disaster affecting the ICT systems, and perhaps assess the organization's approach to risk management (Computer Security Institute, 2003).

ICT management audits are conducted to review the organization, structure, strategy, work planning, resource planning, budgeting, cost controls etc. and, where applicable, relationships with outsourced ICT providers (in some cases, these aspects may be audited by operations and financial auditors, leaving the computer auditors to the more technological aspects). In addition, ICT strategy audits conduct a review of various aspects of ICT strategy, vision and plans, including their relationship to other strategies, visions and plans (Institute of Internal Auditors (IIA), 2000).

Change management aspect of the audit reviews the planning and control of changes to systems, networks, applications, processes, facilities etc., including configuration management, control over the promotion of code from development through testing to production, and the management of changes to the organization as a result of ICT.

Information security and control audit reviews controls relating to confidentiality, integrity and availability of systems and data while "Special investigations" audit involves contingency and un-pre-planned work such as investigating suspected frauds or information security breaches, performing due diligence review of ICT assets for mergers and acquisitions. ICT legal compliance audits checks the legal and regulatory aspects of ICT systems (e.g. software copyright compliance, protection of personal data). It is very important that the legal requirements of licensing of software are adhered to, as failure may lead to court fines, bad public image and even imprisonment (Computer Security Institute, 2003).

Each audit may consist of these elements in varying measures; some audits may scrutinize only one of these elements or drop some of these elements. While the fact remains that it is necessary to do all of them, it is not mandatory to do all of them in one assignment. The skill sets required for each of these are different. The results of each audit need to be seen in relation to the other. This will enable the auditor and management to get the total view of the issues and problems. This overview is critical and hence the essence of ICT auditing (Warren. 2001).

2.8 Risk-based Approach of an ICT Audit Process

Every organization uses a number of information systems. There may be different applications for different functions and activities as well as there being a number of computer installations at different geographical locations. In this case the auditor is faced with the questions of what to audit, when and how frequently. The answer to this is to adopt a risk-based approach. While there are risks inherent to information systems, these risks impact different systems in different ways (Institute of Internal Auditors (IIA), 2000).

The steps that can be followed for a risk-based approach to making an audit plan are taking an inventory of the information systems in use in the organization and categorize them by determining which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate (Le Grand, 2001). This can also be done by an assessment of what risks affect the various systems and the severity of impact on the business and ranking the systems based on the above assessment to make a decision on the audit priority, resources, schedule and frequency.

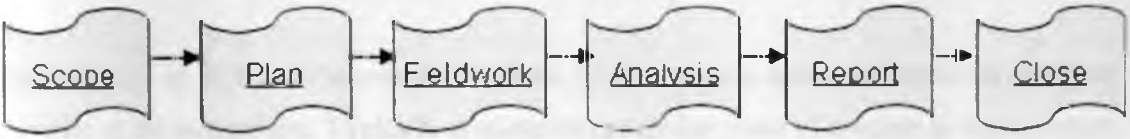
2.9 Application of ICT Audit in Other Audits

The purpose of financial audit is to express an opinion on the financial statements and financial accountability of the business. Most financial and accounting systems are ICT based and hence the overall purpose of the ICT component of a financial audit is to asses the reliability of ICT controls that support the processing of financial records. In this case the ICT auditor should be aware of the risks that the organization face so that focus is made on the areas that pose the greatest risk to the organization not presenting fair and true financial statements (Computer Security Institute. 2003).

Performance audits are conducted to evaluate the efficiency, economy and/or administrative effectiveness of the business. ICT auditing can play a role in examining an organization's ICT systems performance against a benchmark. Secondly, an ICT audit as a component of performance audit will seek to support the work of a performance audit that is focused on efficiency and effectiveness of business processes.

2.10 ICT Auditing Process

Different audit organizations go about computer auditing in different ways and individual auditors have their own preferred ways of working. However the main stages of a "typical" computer audit assignment are as follows (IsecT Institute, 2006)



1. Scoping and pre-audit survey involves the auditor determining the main area/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment. Information sources at this stage include background reading and web browsing, previous audit reports and, sometimes, subjective impressions that deserve further investigation.

2. Planning and preparation for the audit is the stage at which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

3. Fieldwork stage entails gathering evidence by interviewing staff and managers, reviewing documents, printouts and data and observing processes This step may include the use of Computer Aided Audit Techniques (CAATs) to help analyze the IS systems and applications.

4. Analysis stage is about sorting out, reviewing and trying to make sense of all that evidence gathered earlier. It includes undertaking SWOT (Strengths, Weaknesses, Opportunities, Threats) review of the ICT environment.

5. Reporting phase involves reviewing and trying to make sense of the analysis, then writing it up. The preliminary report is then circulated within the department for peer review, modifying it again, then circulating or presenting it to clients and client managers to have their comments and finally issuing it.

6. Closure is the process of sorting out the indexing and cross-referencing and literally shutting the audit files, closure involves preparing notes for future audits and following up on the management to complete the actions of the previous audit. Most organizations however do need to 'close the loop' whereby there really are valid reasons why previously-agreed actions are not undertaken (IsecT Institute, 2006).

2.11 Scope of Computer Audit

The scope of an ICT audit is normally defined by the scoping document produced nearly at the start of the assignment. Typically it relates to certain key risks of concern to management that centre round the computer and/or telecommunications systems. The scope of an audit assignment is normally a balance between breadth (i.e. the range of matters to be reviewed) and depth (i.e. the amount of detail reviewed in each matter). Clever audit plans allow for a bit of both through mixing broadly-scoped high-level audits (designed to find the most important risk areas) with narrowly-scoped in-depth audits (Institute of Internal Auditors (IIA), 2000).

The scope of computer audit is hard to define as it depends on the size and make-up of the audit team: in large audit teams, computer audit may have a number of dedicated and specialized staff solely responsible for technology auditing, but more often the computer auditors are expected to contribute to other types of audit (Institute of Internal Auditors (IIA), 2000).

2.12 Internal and External ICT Audits

External auditors are always employed by a separate organization and are normally contracted by the organization to perform audits as part of the process of preparing company statements (Institute of Internal Auditors (IIA), 2000). In practice, External auditors are mostly employed for a few months a year to examine and provide a formal opinion on the organization's state of financial accounts. Their formal opinion is normally presented in a highly-stylized form in the organization's annual report to shareholders. Computer auditors working for an external audit company are typically concerned with integrity of the client's core financial data and accounting systems (general ledger etc.) and other important systems involved in generating and processing financial records (e.g. sales order processing systems).

Internal Auditors, by contrast, are permanently employed by the organization to examine and comment on its control systems and processes on an ongoing basis, although (as noted earlier) they do not normally report to the organization's conventional executive management structure. Some organizations outsource internal audit to external consultancies but this merely clouds the issue. Their remit usually extends well beyond the core financial systems, encompassing the broader systems of corporate governance (also known as 'management controls'). In some organizations, the external and internal Auditors have separate but complementary areas of scope: External auditors primarily cover the core financial systems whilst internal auditors primarily cover the remainder. In most cases, however, the two functions overlap, working together on some parts (Institute of Internal Auditors (IIA), 2000).

2.13 Key Challenges faced in ICT Audits

IS audit often involves finding and recording observations that are highly technical. Such technical depth is required to perform effective ICT audits. At the same time it is necessary to translate audit findings into vulnerabilities and businesses impacts to which operating managers and senior management can relate.

Budget constraint is usually cited as a major factor limiting the implementation of successful and comprehensive ICT audit among many developing countries. The level of deployment of ICT in itself is limited due to the same reasons and hence subsequent verification of the integrity of the ICT systems through an audit is also less applied (ICT Audit White Paper, 2004).

Infrastructure (Cabling, Data Center Facilities) Hardware (Server, Desktop, Laptop, Storage) pose a major challenge to ICT auditors. Testing of the efficiency, compliance of defined standards, regulation requirements demand that the auditors be well rounded in their skill. Technical skills in networks implementation, maintenance policies, operating systems and administrations as well as knowledge about systems applications and development become necessary if the auditor to present a fair evaluation of the company's ICT infrastructure and systems (ICT Audit White Paper, 2004).

Organization (built-Up, Personnel) and ICT culture are factors that may hinder successful implementation of ICT audits in Kenya. People have a culture of assuming that, if a system has been working well then there is no need to change. Technological advancement has however led to explosion of new threats to ICT based systems and hence the need for continuous testing against most recent standards and benchmarking the ICT systems against global standards.

ICT Deployment and support in most developing countries including Kenya is limited. The level of computerization is still limited compared to that of the technologically advanced developed countries. Globalization and e-commerce dispensation is a great challenge to the developing countries. International standards, ethical and legal requirements have forced businesses to adapt to the changes in the global environment example is the Sarbanes-Oxley act of 2002.

Low competency of use of ICT auditing tools among the ICT auditors results to limited application of these tools in ICT audits. Some of the packages require competent programmers for example sequence query languages for optimum use. These skills are not commonly available among the traditional auditors and hence posing a major challenge to effective ICT auditing.

A major challenge in ICT auditing is the inadequacy of controls in developed applications Application development process should take into account required level of security, however often applications developed in many businesses deviate from the normal application development process and are not thoroughly tested hence deficient in many aspects that ICT audits look at (ICT Audit White Paper, 2004).

Disaster Recovery and Business Continuity is an important component of ICT auditing. In many businesses Disaster Recovery Planning is a theory rather than practice. In most cases, some of the elements of the DRP are not thoroughly tested, there is no simulation of disaster and hence when a catastrophe strikes there is very little continuity of business operations.

The strategic role of ICT is not common knowledge. Few businesses have deployed ICT for strategic purposes. For the businesses where ICT has no strategic role and cases where the need to maintain competitive advantage is not of critical relevance, ICT auditing as a process of evaluation of how IT fits into the overall business strategy does not arise (ICT Audit White Paper, 2004).

ICT Security is of critical importance and should be a consideration to perform an explicit ICT Security Audit. Information security has many elements most of them highly technical and requiring specialized skills not commonly available among many audit teams of many companies. This is an obvious challenge faced in ICT audits in many developing countries.

CHAPTER THREE:

RESEARCH METHODOLOGY

3.1 Research Design

The study was an exploratory survey involving all commercial banks with operations in Nairobi. The design was appropriate considering that not much was known to make it possible to do a more advanced research. The exploratory research was hence used to provide insights into and an understanding of the state of ICT auditing among Kenya's commercial banks. This exploratory research paves way for further descriptive research to define the relevant courses of action on developing an ICT auditing framework for use among Kenyan firms.

3.2 Population

The study was a census and hence the whole population was considered. The target was all the 46 commercial banks with offices in Nairobi (Annex II). A census was appropriate because the target population was small hence manageable. Out of the 46 questionnaires, there was a response of 38 completed questionnaires representing 82.6%. This was found to be adequate for the study findings to be generalized to the target population.

3.3 Data Collection

Pre-testing of the questionnaire was done on a small sample of respondents picked from the target population to identify and eliminate potential problems. This was aimed at refining the questionnaire in-terms of questions content, wording, sequence form and layout, question difficulty, and instructions clarity. The respondents in the pretest were similar to those included in the actual survey in-terms of background characteristics and familiarity with the topic. Corrections and enhancements of the questionnaire were made based on the feedback obtained from the pre-testing. Several ICT audit reports from one of the International commercial banks were also thoroughly analyzed to ensure that the questionnaire adequately captured most aspects of ICT auditing in a bank's environment.

Data collection was done through a structured questionnaire administered through a 'drop and pick' later method. Follow-up was made to ensure collection of the questionnaires on time, as well as assisting respondents who encountered difficulty in completing questionnaires. The respondents were ICT managers, heads of ICT departments and ICT auditors from the internal audit department who were believed to have the knowledge required for the study.

The questionnaire was structured as follows:-

Section A covered general information, demographic information including age and size, number of employees and level of use of ICT systems.

Section B concerned information relating to the extent of ICT audit, functional areas covered by ICT audits and specific elements of ICT audits. This section also gathered information on aspects of ICT auditing including scope and methodology of the ICT audit, periodicity of ICT audits and reporting.

Section C concerned information relating to challenges faced when carrying out ICT audit within banks in Kenya.

3.4 Data Analysis

Completed questionnaires were reviewed and edited for completeness, coded, labeled and keyed into the computer for statistical analysis. Data preparation included checking for acceptable questionnaires, followed by editing, coding and transcribing the data. Questionnaire checking was done whereby a review of all questionnaires for completeness and interviewing quality editing was done to increase accuracy and precision. This included coding of unstructured or open ended questions where by mutually exclusive and collectively exhaustive categories were identified. This ensured that each response fitted into one and only one category code and that every response fits into one of the assigned category codes. Data cleaning was conducted to ensure consistency checks and treatment of missing responses.

Data collected from section A was analyzed using descriptive statistics such as frequency distribution to give general overall picture of the entities under study, level of usage of ICT systems, and variations in size and age.

Data collected from Section B was analyzed though descriptive statistics of frequency tables to indicate the extent of ICT auditing in the various functional areas, specific aspects of focus by ICT audits among the cases.

Section C data was analyzed by factor analysis. Factor analysis is a statistical technique for classifying a large number of interrelated variables into a limited number of factors. The limited number of factors is derived such that the maximum amount of information available in the original variables is retained. The purpose of this analysis was to establish the challenges of ICT auditing from the respondents point of view.

CHAPTER FOUR:

DATA ANALYSIS AND FINDINGS

4.1 Introduction

This chapter presents the results of the analysis and findings of the study. Out of the 46 commercial banks targeted in the study, there were 38 completed questionnaires representing an 82.6 % response. This response rate was considered adequate and representative to allow generalization of the findings.

4.2 Demographic Characteristics

The demographic characteristics of interest were age of the bank, ownership structure and size. These were tested from the respondents providing information about the year of incorporation, bank's ownership structure, approximate number of employees, geographical coverage and the estimated number of accounts held in the bank. Demographic information related to the age of the banks extracted from collected data is summarized in Table 4.1.1. The findings showed that 50 % of the commercial banks were above 20 years since their incorporation.

Table 4.1.1 Distribution of banks by age

	Age of the bank	Frequency	Percent
Valid	Below 10 years	7	18.4
	10 - 20 years	12	31.6
	Above 20 years	19	50.0
	Total	38	100.0

Banks were also categorized in terms of their geographical coverage and on whether local, regional or international. Table 4.1.2 shows the distribution of banks on this criterion. Among the banks, 65.8 % of these had local coverage while only 5 % had a world-wide coverage.

Table 4.1.2 Geographical coverage of commercial banks

Geographical coverage		Frequency	Percent
Valid	Local within	25	65.8
	Regional	8	21.1
	Worldwide	5	13.2
	Total	38	100.0

Closely related to the geographical coverage was the spread of the bank's ICT network as shown in Table 4.1.3. Data shows that 52.6 % of the banks had all over the countrywide network coverage while only 7.9 % had a worldwide coverage. This would suggest that banks with wider network coverage would have to undertake ICT audits to ensure that network infrastructure and systems function as intended.

Table 4.1.3 ICT Network Coverage

ICT Network coverage		Frequency	Percent
Valid	Nairobi	12	31.6
	Countrywide	20	52.6
	Regional	3	7.9
	Worldwide	3	7.9
	Total	38	100.0

Table 4.1.4 shows the distribution of banks by ownership structure. The study findings indicated that 36.8 % of the commercial banks included in the survey are publicly owned, 47.4 % privately owned while only 15.8 % were government owned. In theory, ownership would be a significant determinant of extent of ICT auditing with public owned companies

being expected to undertake the exercise to create more confidence to the shareholders and other stakeholders. Similarly, foreign owned banks would be more vigilant to undertake ICT auditing due to the international outlook and management so as to adhere to the company's international policies.

Table 4.1.4 Distribution by Ownership Structure

	Ownership	Frequency	Percent
Valid	Public	14	36.8
	Private	18	47.4
	Government	6	15.8
	Total	38	100.0

Size of the bank as determined by the number of bank accounts was an important factor analyzed from the data. Table 4.1.5 shows the distribution of banks categorized by the number of bank accounts held. Study findings indicated that 44.7 % of the banks had accounts below 10,000 while only 7.9 % had more than a million bank accounts. The extent of ICT auditing among the banks would have been expected to vary with the variation in number of accounts held.

Table 4.1.5 Distribution of banks by number of bank accounts

		Frequency	Percent
Valid	Below 10,000	17	44.7
	10,000 - 100,000	12	31.6
	100,000 – 1 Million	6	15.8
	Above 1Million	3	7.9
	Total	38	100.0

Bank sizes were also determined on the basis of the number of employees. Analysis showed that 30 out of the 38 banks considered in the study had less than 500 employees while only 4 of the banks had more than 1000 employees. Table 4.1.6 shows the frequency distribution of banks by the number of employees. Variation on level of ICT auditing would be expected to vary accordingly.

Table 4.1.6 Distribution of banks by number of employees

Number of Employees		Frequency	Percent
Valid	Below 500	30	78.9
	500 - 1000	4	10.5
	above 1000	4	10.5
	Total	38	100.0

Responses were also categorized in-terms of whether the bank had a fully pledged IT department or not. Table 4.17 shows that 92 % of the banks had a fully pledged IT department indicating that ICT is now viewed as a critical element of business strategy and governance hence the need for ICT auditing. Only three banks representing 8 % of the respondents had their ICT activities being managed under the finance department.

Table 4.1.7 Distribution of banks by fully pledged IT departments

Fully pledged IT dept.		Frequency	Percent
Valid	Yes	35	92.1
	No	3	7.9
	Total	38	100.0

Table 4.1.8 shows the distribution of the banks based on whether they had internal auditing departments. Study findings showed that 94.7 % of the banks had an internal audit department while only 5.3 % did not. Banks with internal audit department would easily engage in ICT auditing as compared to those that did not have. Amongst the banks with

internal audit departments, there were variations in terms of the number of internal auditors ranging between one and 18.

Table 4.1.8 Bank with Internal Audit department

		Frequency	Percent
Valid	Yes	36	94.7
	No	2	5.3
	Total	38	100.0

Frequency of ICT auditing by the banks was also considered. In view of this, results from Table 4.1.9 show that most ICT auditing in commercial banks in Kenya is conducted continuously by internal audit departments. The study found that 60.5 % of the respondents undertook their ICT audits continuously, 23.7 % had their ICT audits annually while only 5.3 % had ad-hoc ICT audits.

Table 4.1.9 Distribution of banks by frequency of ICT audits

Frequency of ICT audits		Frequency	Percent
Valid	Once a year	9	23.7
	Twice a year	4	10.5
	Continuously	23	60.5
	Ad-hoc	2	5.3
	Total	38	100.0

The study showed that ICT audits in commercial banks in Kenya are mainly performed by the bank's internal auditors while the rest do undertake their ICT audits through audit firms and consultants. However international and foreign owned banks had ad-hoc ICT audits conducted by the company group audit teams. Most respondents indicated that the reference for authoritative auditing is made from both company guidelines and international auditing guidelines.

4.3 Extent of ICT Auditing

The respondents were asked to indicate the extent to which the banks ICT audit focused on the various aspects of confidentiality, Integrity and Availability. This was in line with the first objective of the study. The findings showed ICT audits were extensively focusing on the availability of ICT systems and services. This was in line with what had been observed in the pre-testing and the ICT audit reports from Standard Chartered Bank. Table 4.2.1 shows the study findings on extent of ICT auditing on availability of ICT systems and services.

Table 4.2.1 Extent of ICT audit on ICT systems availability

	Extent of focus on availability	Frequency	Percent
Valid	No extent	2	5.3
	Less Extent	5	13.2
	Moderate Extent	8	21.1
	Great Extent	11	28.9
	Greatest Extent	12	31.6
	Total	38	100.0

The study found that systems availability was the most critical area that ICT audits focused on. The results showed 31.6 % of banks systems availability had received the greatest extent of focus during the bank's ICT auditing. From the ICT audit report 2003 for Standard Chartered Bank, ICT auditors focused more on the availability of ATM services and the banking operations systems than most of the other areas of the bank.

More evidence of greatest extent of ICT audits on services availability was shown by the respondents view on the extent of ICT auditing on systems downtime, systems backup procedures and Disaster Recovery Planning. These aspects are aimed at ensuring that ICT systems are available for use as when required. According to the study findings, 55.3 % of the banks had a greatest extent of focus on systems downtimes as compared to only 10% who indicated less extent of focus on this aspect. The results of systems downtimes are shown on Table 4.2.2

Table 4.2.2 Extent of ICT audit on systems downtimes

Focus on system downtimes		Frequency	Percent
Valid	Less Extent	4	10.5
	Moderate Extent	3	7.9
	Great Extent	10	26.3
	Greatest Extent	21	55.3
	Total	38	100.0

Disaster Recovery Planning is closely related to ICT services availability. It is a key element of the overall Business Continuity Planning. Disaster Recovery Planning is aimed at ensuring that the business continues to operate in the event of a disaster. Implementation of DRP is through efficient system backups, redundancy in the infrastructure and systems. Table 4.2.3 shows the study findings relating to the extent of ICT auditing on Disaster Recovery Plans. The study found that 42.1 % of the respondents viewed DRP audits having received greatest extent of focus during their bank's audits while only 7% viewed the bank's ICT audits as having no extent of focus on the DRP issues.

Table 4.2.3 Extent of ICT audits on Disaster recovery planning

		Frequency	Percent
Valid	No extent	3	7.9
	Less Extent	2	5.3
	Moderate Extent	6	15.8
	Great Extent	11	28.9
	Greatest Extent	16	42.1
	Total	38	100.0

ICT security is a critical factor in bank's ICT audit. The study indicated more than 70 % of the respondents viewed ICT security has having at-least a great extent of focus during the bank's ICT audits. Table 4.2.4 summarizes the study findings on the extent of ICT audits on ICT security.

Table 4.2.4 Extent of ICT Audit on Security

		Frequency	Percent
Valid	No extent	4	10.5
	Less Extent	1	2.6
	Moderate Extent	5	13.2
	Great Extent	13	34.2
	Greatest Extent	15	39.5
	Total	38	100.0

A major concern of banks today regarding to their computer systems is how to guarantee the confidentiality and integrity of the various day to day processes on which their organizations are increasingly more dependent. This is doubtless one of the greatest challenges faced by ICT professionals. The importance of ICT logical controls in audits was found to be critical during ICT audits with more than 44 % of the respondents indicating that logical controls received a greatest extent attention. More than 80% of the respondents were cumulatively above the moderate extent level. Table 4.2.5 shows the findings of the study on extent of focus on logical controls.

Table 4.2.5 Extent of focus on logical controls

		Frequency	Percent
Valid	No extent	3	7.9
	Less Extent	4	10.5
	Moderate Extent	5	13.2
	Great Extent	9	23.7
	Greatest Extent	17	44.7
	Total	38	100.0

In addition, respondents were asked about the extent to which the bank's ICT audits focused on general controls and the findings summarized in Table 4.2.6. Study findings showed 52.6% of the respondents indicated that controls received a greatest extent of focus during ICT audits.

Table 4.2.6 Extent of ICT auditing on Controls

		Frequency	Percent
Valid	Less Extent	1	2.6
	Moderate Extent	6	15.8
	Great Extent	11	28.9
	Greatest Extent	20	52.6
	Total	38	100.0

4.4 Factor Analysis of the challenges faced in ICT Auditing in Banks

This section addresses the second objective of the study, which is to determine the challenges faced in ICT auditing in banks. Factor analysis was performed on the results of the extent to which different factors were a challenge to the implementation of successful auditing in banks. Factor analysis is a technique applicable where there is a systematic interdependence among a set of observed or manifest variables and the researcher is interested in finding out something more fundamental or latent which creates commonality. Thus factor analysis seeks to resolve a large set if measured variables in-terms of relatively few categories known as factors. Table 4.2.7 shows the list of variables that were considered for analysis.

Table 4.2.7 List of variables of challenges faced in ICT audits

F1. Few numbers of users with computerized systems
F2. Lack of trained and qualified staff
F3. Complexity of ICT exercise
F4. Lack of cooperation from internal departments
F5. High training costs
F6. High cost of acquisition of computers and associated software
F7. Lack of ICT audit guidelines
F8. Challenges of coping with technology changes
F9. Lack of management appreciation of the importance of ICT auditing
F10. Budget constraints
F11. Poor assessments of threats and vulnerabilities
F12. Lack of awareness about ICT auditing
F13. Interpretation of ICT audit findings by senior managers
F14. Challenges due to complexity of ICT infrastructures
F15. Poorly defined compliance framework (standards, copyrights)
F16. Lack of standardized ICT audit framework/guidelines
F17. ICT culture that ICT systems will always work well
F18. Conflict of interest
F19. Lack independence of auditors as they perform ICT audits
F20. Time constraints
F21. Destruction of ICT audit trails by the auditee
F22. Problems with ICT audit Scope definition
F23. Unavailability of data required by the ICT auditor

F24. Lack of ICT auditing skills
F25. Difficulties in identification of ICT risks
F26. Limited management support and commitment
F27. Interconnectivity to customers' and suppliers' systems and outsourcing of ICT
F28. Poor usage of Computer Aided Audit Tools in ICT auditing
F29. Translation of ICT audit findings into business impacts that managers can relate
F30. Translation of ICT audit findings into vulnerabilities that managers can relate

Correlation Matrix

All respondents that were sampled out indicated the extent to which given factors had contributed to the hindrance of successful ICT audit implementation in banks. Factor analysis grouped the challenges that are very similar to each other into more meaningful classes. By grouping variables with similar characteristics together, the result is a small number of variables that make it easy for the researcher to explain the observed variance in relation to the large number of variables. Correlation is a statistical procedure which is used to explain the relationship and the strength of such a relationship between variables. This is achieved by providing a correlation matrix giving correlations between all pairs of data. The matrix is a rectangular array of elements set out by rows and columns. Existence of clusters of large correlation between subsets of the variables suggests that the variables measure aspects of the same underlying dimension. Usually, the correlation matrix is reduced down to its component dimensions by looking for variables that correlate highly with a group of other variables outside that group.

Table 4.2.8 shows the correlation matrix of the challenges considered important in ICT auditing implementation in commercial banks in view of the respondents. For this particular case, the extraction method used was primary component analysis which seeks to maximize the sum of squared loadings of each factor extracted in-turn. Primary component analysis constructs out of a given set of variables new variables called principal components, which are linear combinations.

Table 4.2.8 Correlation matrix

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15	F16	F17	F18	F19	F20	F21	F22	F23	F24	F25	F26	F27	F28	F29	F30
F1	1	0.304	0.29	0.66	0.37	0.518	0.32	0.21	0.28	0.35	0.27	0.22	0.13	0.152	0.171	0.292	0.35	0.28	-0.07	0.21	0.28	0.24	0.163	0.136	0.35	0.303	0.283	0.31	0.32	0.32
F2	0.3	1	0.7	0.61	0.67	0.72	0.44	0.345	0.62	0.57	0.446	0.44	0.45	0.399	0.364	0.494	0.36	0.4	-0.05	0.31	0.37	0.29	0.192	0.38	0.53	0.345	0.348	0.48	0.453	0.36
F3	0.29	0.7	1	0.46	0.61	0.5	0.5	0.384	0.43	0.37	0.212	0.3	0.27	0.163	0.153	0.358	0.19	0.21	-0.25	0.13	0.23	0.19	0.261	0.318	0.55	0.306	0.286	0.36	0.248	0.16
F4	0.66	0.605	0.46	1	0.71	0.781	0.39	0.316	0.53	0.57	0.493	0.47	0.36	0.332	0.293	0.595	0.54	0.44	0.036	0.41	0.51	0.41	0.338	0.365	0.6	0.469	0.362	0.41	0.59	0.36
F5	0.37	0.667	0.61	0.71	1	0.83	0.46	0.479	0.63	0.56	0.391	0.57	0.32	0.365	0.22	0.518	0.35	0.42	0.069	0.37	0.52	0.46	0.488	0.617	0.71	0.523	0.437	0.59	0.603	0.51
F6	0.52	0.72	0.5	0.78	0.83	1	0.57	0.537	0.74	0.71	0.534	0.66	0.46	0.56	0.373	0.55	0.44	0.57	-0.02	0.44	0.53	0.44	0.349	0.548	0.69	0.614	0.586	0.62	0.697	0.57
F7	0.32	0.442	0.5	0.39	0.46	0.566	1	0.449	0.57	0.46	0.293	0.37	0.38	0.43	0.183	0.307	0.27	0.19	-0.16	0.4	0.38	0.29	0.287	0.292	0.44	0.393	0.438	0.43	0.419	0.32
F8	0.21	0.345	0.38	0.32	0.48	0.537	0.45	1	0.59	0.41	0.442	0.43	0.36	0.405	0.243	0.297	0.21	0.36	-0.16	0.39	0.21	0.29	0.27	0.381	0.39	0.556	0.497	0.49	0.374	0.41
F9	0.28	0.618	0.43	0.53	0.63	0.736	0.57	0.592	1	0.76	0.55	0.68	0.48	0.643	0.382	0.474	0.47	0.48	0.074	0.58	0.59	0.39	0.371	0.367	0.56	0.52	0.509	0.59	0.521	0.49
F10	0.35	0.574	0.37	0.57	0.56	0.705	0.46	0.407	0.76	1	0.423	0.47	0.39	0.503	0.332	0.465	0.48	0.42	0.156	0.46	0.56	0.29	0.374	0.356	0.47	0.371	0.539	0.45	0.496	0.4
F11	0.27	0.446	0.21	0.49	0.39	0.534	0.29	0.442	0.55	0.42	1	0.78	0.66	0.706	0.505	0.618	0.55	0.52	0.176	0.26	0.34	0.13	-0.06	0.076	0.19	0.269	0.265	0.15	0.319	0.13
F12	0.22	0.436	0.3	0.47	0.57	0.659	0.37	0.425	0.68	0.47	0.783	1	0.68	0.787	0.604	0.738	0.68	0.68	0.099	0.35	0.41	0.25	0.179	0.234	0.39	0.408	0.346	0.4	0.403	0.28
F13	0.13	0.451	0.27	0.36	0.32	0.459	0.38	0.356	0.48	0.39	0.66	0.68	1	0.683	0.689	0.623	0.43	0.49	0.096	0.19	0.18	0.05	0.012	-0.01	0.16	0.206	0.139	0.18	0.156	0.1
F14	0.15	0.399	0.16	0.33	0.37	0.56	0.43	0.405	0.64	0.5	0.706	0.79	0.68	1	0.517	0.666	0.58	0.59	-0.05	0.47	0.25	0.11	0.094	0.06	0.28	0.213	0.268	0.31	0.327	0.22
F15	0.17	0.384	0.15	0.29	0.22	0.373	0.18	0.243	0.38	0.33	0.505	0.6	0.69	0.517	1	0.699	0.53	0.72	-0.02	0.34	0.32	0.25	0.114	0.072	0.2	0.349	0.231	0.28	0.284	0.21
F16	0.29	0.494	0.36	0.6	0.52	0.55	0.31	0.297	0.47	0.47	0.618	0.74	0.62	0.666	0.699	1	0.75	0.75	-0.06	0.43	0.39	0.24	0.214	0.175	0.42	0.383	0.365	0.38	0.43	0.27
F17	0.35	0.363	0.19	0.54	0.35	0.437	0.27	0.214	0.47	0.48	0.548	0.68	0.43	0.58	0.526	0.746	1	0.7	0.109	0.51	0.41	0.34	0.387	0.229	0.38	0.307	0.265	0.35	0.375	0.28
F18	0.28	0.401	0.21	0.44	0.42	0.566	0.19	0.359	0.48	0.42	0.518	0.68	0.49	0.592	0.721	0.747	0.7	1	0.157	0.53	0.42	0.35	0.325	0.293	0.42	0.542	0.386	0.49	0.482	0.49
F19	-0.07	-0.05	-0.25	0.04	0.07	-0.02	-0.16	-0.16	0.07	0.16	0.176	0.1	0.1	-0.05	-0.02	-0.06	0.11	0.16	1	0.06	0.3	0.26	0.283	-0.06	-0.19	-0.04	-0.14	-0.12	-0	0.15
F20	0.21	0.308	0.13	0.41	0.37	0.437	0.4	0.388	0.58	0.46	0.258	0.35	0.19	0.466	0.335	0.431	0.51	0.53	0.055	1	0.57	0.39	0.481	0.23	0.5	0.422	0.411	0.5	0.621	0.57
F21	0.28	0.368	0.23	0.51	0.52	0.531	0.38	0.205	0.59	0.58	0.335	0.41	0.18	0.253	0.323	0.391	0.41	0.42	0.302	0.57	1	0.56	0.484	0.407	0.58	0.375	0.626	0.59	0.704	0.65
F22	0.24	0.291	0.19	0.41	0.46	0.441	0.29	0.285	0.39	0.29	0.131	0.25	0.05	0.109	0.245	0.24	0.34	0.35	0.26	0.39	0.56	1	0.71	0.523	0.42	0.56	0.271	0.26	0.608	0.6
F23	0.16	0.192	0.26	0.34	0.49	0.349	0.29	0.27	0.37	0.37	-0.06	0.18	0.01	0.094	0.114	0.214	0.39	0.33	0.283	0.48	0.48	0.71	1	0.566	0.61	0.431	0.307	0.33	0.526	0.54
F24	0.14	0.38	0.32	0.37	0.62	0.548	0.29	0.381	0.37	0.36	0.076	0.23	-0.01	0.06	0.072	0.175	0.23	0.29	-0.06	0.23	0.41	0.52	0.566	1	0.63	0.667	0.465	0.51	0.502	0.49
F25	0.35	0.526	0.55	0.6	0.71	0.686	0.44	0.391	0.56	0.47	0.194	0.39	0.16	0.277	0.199	0.417	0.38	0.42	-0.19	0.5	0.58	0.42	0.614	0.626	1	0.506	0.705	0.67	0.716	0.61
F26	0.3	0.345	0.31	0.47	0.52	0.614	0.39	0.556	0.52	0.37	0.269	0.41	0.21	0.213	0.349	0.383	0.31	0.54	-0.04	0.42	0.38	0.56	0.431	0.667	0.51	1	0.553	0.55	0.533	0.44
F27	0.28	0.348	0.29	0.36	0.44	0.586	0.44	0.497	0.51	0.54	0.265	0.35	0.14	0.268	0.231	0.365	0.27	0.39	-0.14	0.41	0.63	0.27	0.307	0.465	0.71	0.553	1	0.74	0.617	0.57
F28	0.31	0.477	0.36	0.41	0.59	0.62	0.43	0.494	0.59	0.45	0.151	0.4	0.18	0.308	0.28	0.376	0.35	0.49	-0.12	0.5	0.59	0.26	0.325	0.507	0.67	0.551	0.738	1	0.524	0.61
F29	0.32	0.453	0.25	0.59	0.6	0.697	0.42	0.374	0.52	0.5	0.319	0.4	0.16	0.327	0.284	0.43	0.38	0.48	-0	0.62	0.7	0.61	0.526	0.502	0.72	0.533	0.617	0.52	1	0.79
F30	0.32	0.362	0.16	0.36	0.51	0.568	0.32	0.412	0.49	0.4	0.132	0.28	0.1	0.222	0.208	0.266	0.28	0.49	0.146	0.57	0.65	0.6	0.544	0.491	0.61	0.441	0.567	0.61	0.79	1

The Communalities

Communalities show the amount of variance in the variables that has been accounted for by the extracted factors. Each challenge has associated with it a variance reflecting the variation of respondents. The amount of variance for each factor that is accounted for by a specific factor is the communality of the variable. In this case communalities therefore are the percentage of a challenge variance that contributes to the correlation with other challenges. Table 4.2.9 shows the communalities calculated. From the table, it is evident that each of the challenges has a relatively high communality. This therefore suggests that most of the outlined challenges belong to some clusters.

Table 4.2.9 Communalities

Communalities

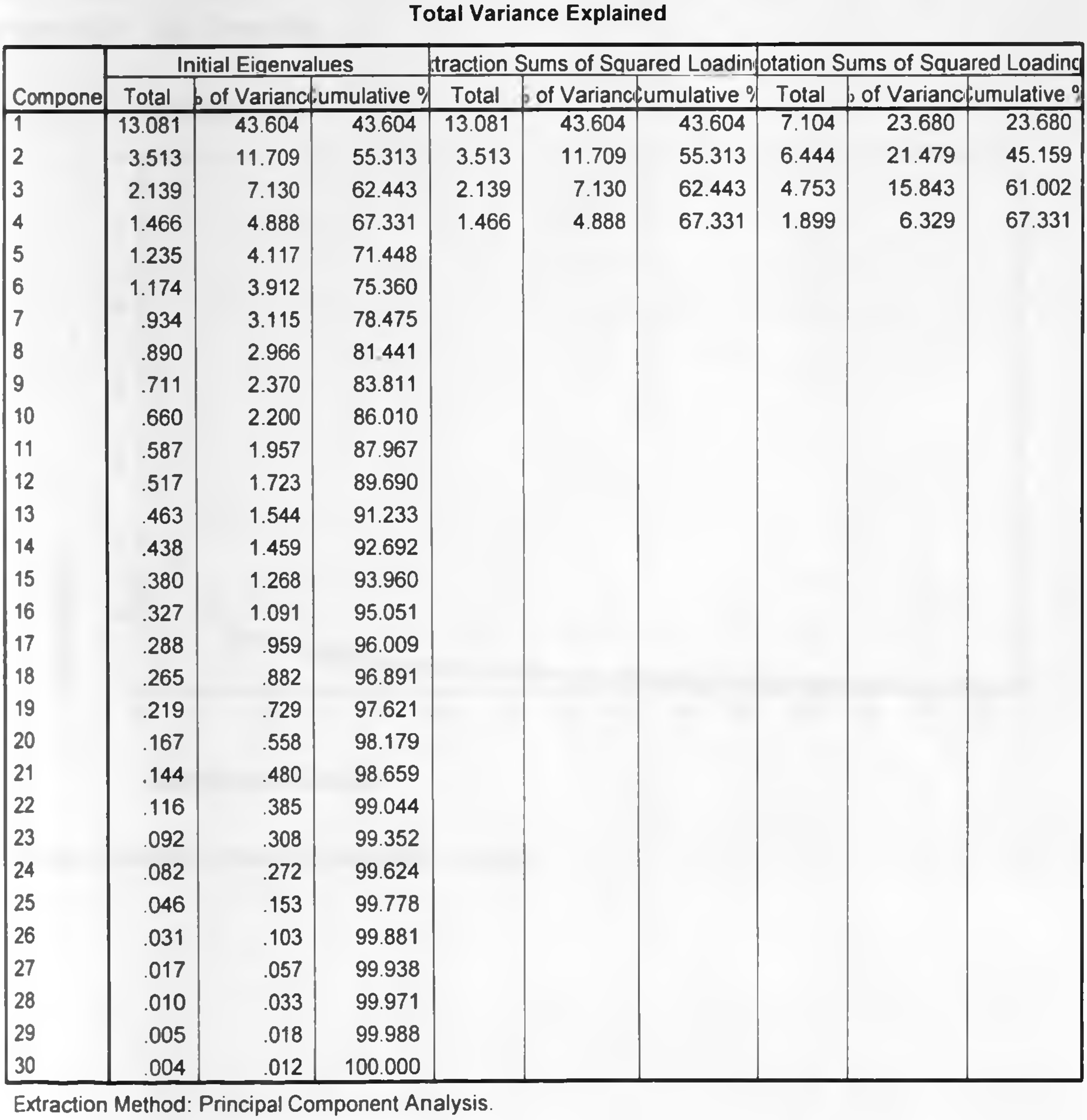
	Initial	Extraction
Fewer no. with comps	1.000	.355
lack of trained and qualified	1.000	.696
complexity of excercise	1.000	.694
lack of cooperation	1.000	.768
high training costs	1.000	.793
high cost of acq of comps	1.000	.861
lack of audit guideliness	1.000	.474
coping with tech changes	1.000	.537
lack mgt appreciation	1.000	.694
budget constraints	1.000	.559
poor assessment of threats	1.000	.724
lack of awareness of	1.000	.804
interpretation of findings by mgrs	1.000	.717
complex ICT infrastructure	1.000	.768
poorly defined compliance	1.000	.634
lack of framework	1.000	.737
ICT culture	1.000	.645
conflict of interest	1.000	.739
lack of independence	1.000	.643
time contraints	1.000	.588
destruction of audit trails	1.000	.666
scope definition	1.000	.670
unavailability of data to auditors	1.000	.680
lack of skills	1.000	.580
difficulty in identifying risks	1.000	.762
limited mgt support	1.000	.550
interdependency of customers	1.000	.704
poor use of CAATs	1.000	.707
translation of ICT audit findings to impacts	1.000	.728
translation of finings to vulnerabilities	1.000	.722

Extraction Method: Principal Component Analysis.

Factor extraction

Table 4.3.0 shows all the factors extracted from the analysis along with their Eigen values, the percent of variance attributed to each factor and the cumulative variance of the factor and the previous factors. In this respect, the first challenge accounts for 43.604% of the variance, the second 11.709% and the third 7.130% and the fourth 4.888% respectively. The rest of the factors are hence insignificant.

Table 4.3.0 Total variance explained



Total Variance Explained

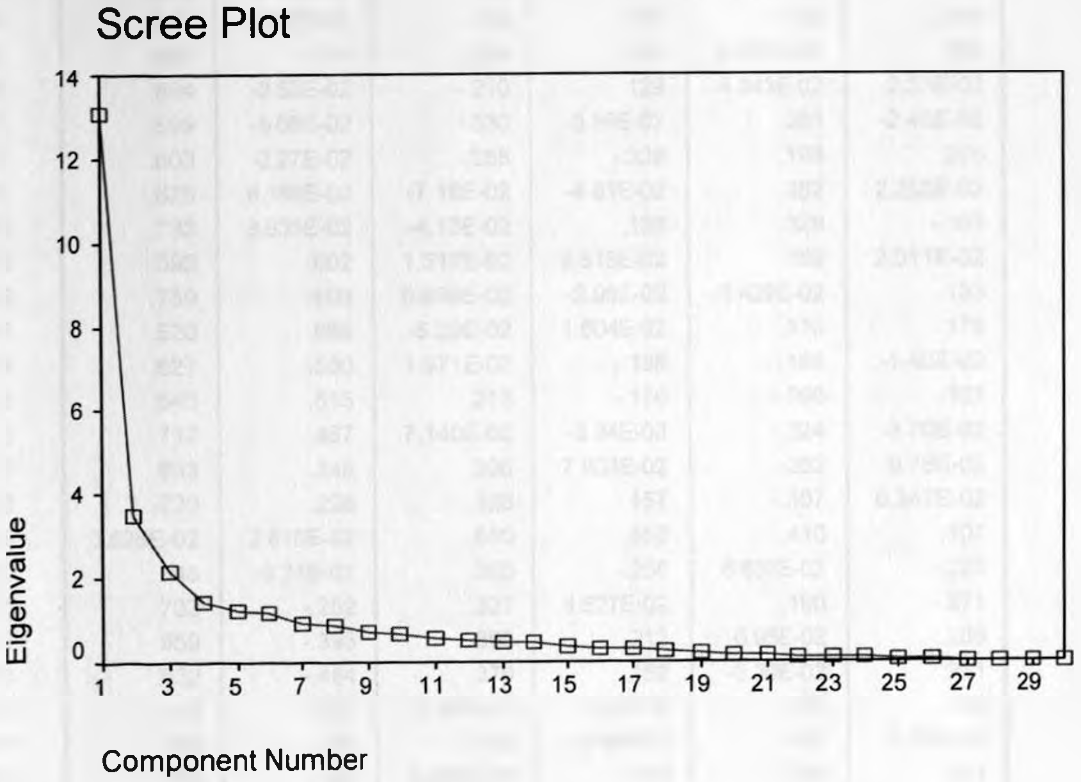
	Initial Eigenvalues			traction Sums of Squared Loadin			otation Sums of Squared Loading		
Compone	Total	of Varianc	umulative %	Total	of Varianc	umulative %	Total	of Varianc	umulative %
1	13.081	43.604	43.604	13.081	43.604	43.604	7.104	23.680	23.680
2	3.513	11.709	55.313	3.513	11.709	55.313	6.444	21.479	45.159
3	2.139	7.130	62.443	2.139	7.130	62.443	4.753	15.843	61.002
4	1.466	4.888	67.331	1.466	4.888	67.331	1.899	6.329	67.331
5	1.235	4.117	71.448						
6	1.174	3.912	75.360						
7	.934	3.115	78.475						
8	.890	2.966	81.441						
9	.711	2.370	83.811						
10	.660	2.200	86.010						
11	.587	1.957	87.967						
12	.517	1.723	89.690						
13	.463	1.544	91.233						
14	.438	1.459	92.692						
15	.380	1.268	93.960						
16	.327	1.091	95.051						
17	.288	.959	96.009						
18	.265	.882	96.891						
19	.219	.729	97.621						
20	.167	.558	98.179						
21	.144	.480	98.659						
22	.116	.385	99.044						
23	.092	.308	99.352						
24	.082	.272	99.624						
25	.046	.153	99.778						
26	.031	.103	99.881						
27	.017	.057	99.938						
28	.010	.033	99.971						
29	.005	.018	99.988						
30	.004	.012	100.000						

Extraction Method: Principal Component Analysis.

The Scree Plot

Figure 4.3.0 is a graph of the Eigen values plotted against all factors. A scree plot helps us to know which factors to maintain and those to leave out as far as our model is concerned. The critical point is usually where the graph starts to flatten. As seen in the figure below, the graph starts to flatten after factors 6 and 7. Factor 6 has an Eigen value of more than one while factor seven has an Eigen value of less than one. We thus drop factor 7 but consider factor 6. This is indeed a confirmation that only six factors are considered important in the analysis

Figure 4.3.0 The Scree Plot



Extraction Method: Principal Component Analysis

Factor matrix

Once factors have been extracted, the loadings of the challenges on each factor are calculated. The higher the absolute value of the factor loading, the greater that particular challenge contributes to the variable.

Table 4.3.1 Component Matrix

Component Matrix [a]

	Component					
	1	2	3	4	5	6
F1	.464	-4.94E-02	-.172	.328	-.286	-.456
F2	.697	7.461E-02	-.359	.275	3.931E-02	4.460E-02
F3	.520	-7.69E-02	-.589	.266	-7.53E-02	.168
F4	.748	4.777E-03	-.125	.438	-.190	-.218
F5	.801	-.174	-.204	.282	2.030E-02	.153
F6	.894	-2.52E-02	-.210	.129	4.343E-02	-2.33E-02
F7	.599	-5.08E-02	-.330	-5.56E-02	.281	-2.46E-02
F8	.603	-2.27E-02	-.255	-.329	.198	.295
F9	.825	8.186E-02	-7.18E-02	-4.61E-02	.382	2.253E-02
F10	.733	3.935E-02	-4.13E-02	.136	.329	-.161
F11	.593	.602	1.517E-02	9.515E-02	.159	2.011E-02
F12	.739	.503	6.989E-02	-2.98E-02	3.429E-02	.133
F13	.520	.665	-5.29E-02	1.604E-02	.115	.175
F14	.627	.580	1.971E-02	-.195	.185	-1.40E-02
F15	.540	.515	.213	-.176	-.290	.101
F16	.717	.467	7.140E-02	-3.34E-03	-.324	-3.70E-02
F17	.653	.346	.305	7.903E-02	-.262	-9.78E-02
F18	.720	.298	.328	-.157	-.307	6.347E-02
F19	3.628E-02	2.815E-02	.660	.453	.410	.101
F20	.648	-9.31E-02	.306	-.256	8.637E-02	-.225
F21	.703	-.252	.327	4.527E-02	.190	-.271
F22	.559	-.393	.398	.212	-6.95E-02	.285
F23	.532	-.484	.370	.162	-3.39E-02	.251
F24	.566	-.507	-5.46E-02	-1.42E-02	-.139	.398
F25	.766	-.385	-.155	-5.48E-02	-.152	-7.99E-02
F26	.678	-.240	3.036E-03	-.179	-.199	.341
F27	.671	-.289	-.109	-.397	6.157E-02	-.223
F28	.709	-.267	-.127	-.341	-1.16E-02	-.149
F29	.766	-.327	.173	-6.34E-02	-2.92E-02	-.169
F30	.665	-.426	.275	-.152	6.663E-02	-.123

Extraction Method: Principal Component Analysis.

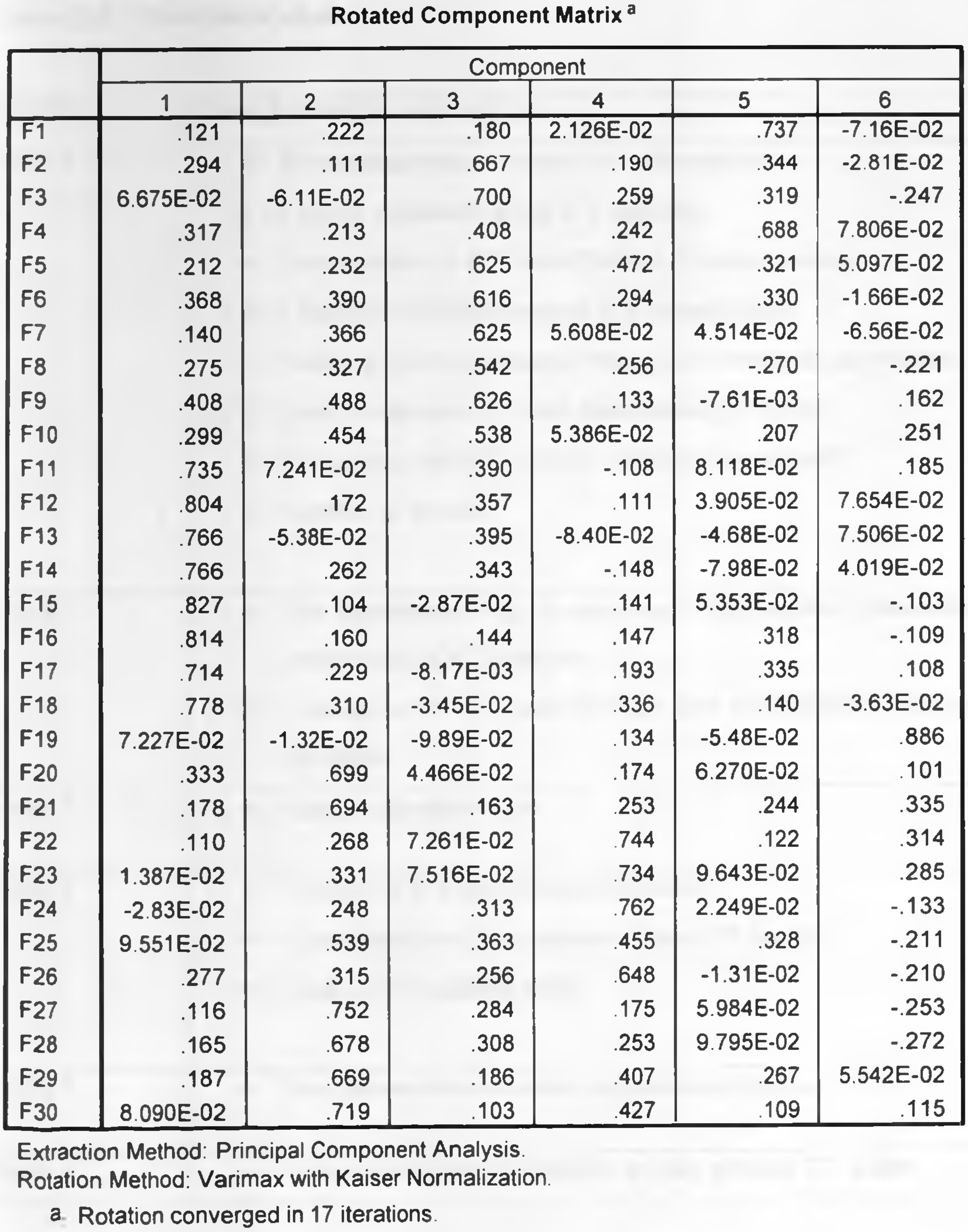
a. 6 components extracted.

Table 4.3.1 shows the component matrix of the variables of challenges faced in effort towards successful ICT auditing in commercial banks.

Factor Rotation

Factor rotation procedure is aimed at reducing the number of factors on which the variables under investigation have high loadings. This only acts to make interpretation easier as shown in Table 4.3.2.

Table 4.3.2 Rotated component matrix



Rotated Component Matrix [a]

	Component					
	1	2	3	4	5	6
F1	.121	.222	.180	2.126E-02	.737	-7.16E-02
F2	.294	.111	.667	.190	.344	-2.81E-02
F3	6.675E-02	-6.11E-02	.700	.259	.319	-.247
F4	.317	.213	.408	.242	.688	7.806E-02
F5	.212	.232	.625	.472	.321	5.097E-02
F6	.368	.390	.616	.294	.330	-1.66E-02
F7	.140	.366	.625	5.608E-02	4.514E-02	-6.56E-02
F8	.275	.327	.542	.256	-.270	-.221
F9	.408	.488	.626	.133	-7.61E-03	.162
F10	.299	.454	.538	5.386E-02	.207	.251
F11	.735	7.241E-02	.390	-.108	8.118E-02	.185
F12	.804	.172	.357	.111	3.905E-02	7.654E-02
F13	.766	-5.38E-02	.395	-8.40E-02	-4.68E-02	7.506E-02
F14	.766	.262	.343	-.148	-7.98E-02	4.019E-02
F15	.827	.104	-2.87E-02	.141	5.353E-02	-.103
F16	.814	.160	.144	.147	.318	-.109
F17	.714	.229	-8.17E-03	.193	.335	.108
F18	.778	.310	-3.45E-02	.336	.140	-3.63E-02
F19	7.227E-02	-1.32E-02	-9.89E-02	.134	-5.48E-02	.886
F20	.333	.699	4.466E-02	.174	6.270E-02	.101
F21	.178	.694	.163	.253	.244	.335
F22	.110	.268	7.261E-02	.744	.122	.314
F23	1.387E-02	.331	7.516E-02	.734	9.643E-02	.285
F24	-2.83E-02	.248	.313	.762	2.249E-02	-.133
F25	9.551E-02	.539	.363	.455	.328	-.211
F26	.277	.315	.256	.648	-1.31E-02	-.210
F27	.116	.752	.284	.175	5.984E-02	-.253
F28	.165	.678	.308	.253	9.795E-02	-.272
F29	.187	.669	.186	.407	.267	5.542E-02
F30	8.090E-02	.719	.103	.427	.109	.115

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 17 iterations.

Isolation of challenges for each factor

Isolation of challenges for each factor involves isolating each challenge that constitutes each factor based on the factor loadings. These are the correlation between the factors and the challenges encountered. Table 4.3.3 shows the challenges for each factor based on a minimum correlation of 0.7 for the isolation of the key challenges.

Table 4.3.3 Isolation of challenges

FACTOR	CHALLENGES/ VARIABLES
Factor 1	• Poor assessments of threats and vulnerabilities • Lack of awareness about ICT auditing • Interpretation of ICT audit findings by senior managers • Challenges of complexity of ICT infrastructure • Poorly defined compliance framework (standards, copyrights) • Lack of standard ICT audit framework/guidelines • ICT culture that ICT systems will always work well • Conflict of interest
Factor 2	• The interconnectivity to customers' and suppliers' processing and outsourcing of ICT services • Translation of ICT audit findings into vulnerabilities that managers can relate
Factor 3	• Complexity of exercise
Factor 4	• Problem of ICT audit Scope definition • Unavailability of data required by the ICT auditor • Lack of ICT auditing skills
Factor 5	• Few numbers of users with computerized system
Factor 6	• Lack independence of auditors as they perform ICT audits

Factor 1 is where most of the challenges were classified. These challenges were those related to poor assessment of threats and vulnerabilities, lack of awareness about ICT auditing, interpretation of ICT audit findings by senior managers, complexity of ICT infrastructure, poorly defined compliance framework (standards, copyrights) and the lack of standard ICT audit framework/guidelines. Challenges resulting from organizations ICT culture that ICT systems would always work well and conflict of interest were also classified under factor 1.

Factor 2 indicated challenges related to the interconnectivity to customers' and suppliers' processing systems and outsourcing of ICT services as well as challenges of translation of ICT audit findings into vulnerabilities that managers can relate. These were also cited as critical challenges that were being encountered in effort to ICT auditing in commercial banks sampled.

Factor 3 was related to the challenge of the complexity of the ICT auditing exercise.

Factor 4 challenges relate to problems of ICT audit scope definition, unavailability of data required by the ICT auditors and lack of ICT auditing skills among the conventional audit teams.

Factor 5 is related to challenges of fewer numbers of users with computerized system.

Factor 6 is concerned with the lack of independence of auditors as they perform ICT audits thus compromising the standards of ICT auditing due to other parties interfering with the process.

Table 4.3.4 Component transformation matrix

Component Transformation Matrix

Component	1	2	3	4	5	6
1	.524	.524	.483	.388	.258	.017
2	.768	-.372	.019	-.515	-.067	.039
3	.248	.225	-.664	.246	-.128	.609
4	-.134	-.482	.227	.120	.608	.560
5	-.203	.241	.480	-.355	-.480	.560
6	.121	-.496	.208	.619	-.559	-.008

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

4.4 Conclusions

The main aim of the study was to obtain and analyze quantitative data to reveal the real situation of Kenya's commercial banks with regard to ICT auditing and the main challenges that are faced towards successful implementation of ICT audits. This exploratory research provided a basis for more in-depth studies into the issue. Nevertheless, from the study some pertinent conclusions from the data gathered provided some insight into the extent to which ICT auditing has been adopted in Kenya and the challenges being experienced in the effort to successful ICT auditing. Most of the challenges faced were found to be relating to poor assessment of threats and vulnerabilities, lack of awareness about ICT auditing, interpretation of ICT audit findings by senior managers, complexity of ICT infrastructure, poorly defined compliance framework (standards, copyrights), lack of standard ICT audit framework/guidelines and the organization's ICT Culture that ICT systems always work well.

CHAPTER FIVE:

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

In this chapter, study results are summarized, then conclusions arrived at from the research findings are discussed in light of the objectives of the study and finally, recommendations made. The study sought to identify the extent of ICT auditing among the commercial banks in Kenya and the challenges that are faced in the effort towards successful implementation of ICT auditing. Data from the completed questionnaires was analyzed primarily by the use of descriptive statistical measures such as frequency and factor analysis.

The results analyzed relate to 38 respondents out of entire population of 46 commercial banks in Kenya. From the study findings it was found that commercial banks do undertake ICT audits and at varied extents in terms of the areas of focus. ICT systems and services availability, confidentiality and integrity are extensively addressed in most of the audits being conducted across the banks. The frequency at which respondent banks undertook ICT audits indicated that ICT is viewed as an important area of governance in the banking sector. Most banks undertake their ICT audits continuously while a few do it annually.

5.2 Summary and conclusions

As per the study objectives, the study was successful in that it established the extent of ICT auditing in commercial banks in Kenya and outlined the challenges that face successful implementation of ICT audits.

The banking sector in Kenya is fast growing as shown by the number of the commercial banks, geographical coverage and the extent of their ICT networks. Also noted from the study was that most of the bank's operations and functions are computerized and hence the need for ICT auditing. The concept of ICT auditing is practiced extensively with great variations among the banks on the extent and focus given to each of the areas of Availability, confidentiality and integrity. Challenges commonly faced were related to poor assessments of threats and vulnerabilities and the lack of awareness about ICT auditing especially among the small banks. poor interpretation of ICT audit findings by the management hence resulting to inadequate support.

Findings of the study indicated that most of the commercial banks in Kenya were aware of and conducted ICT audits regularly. ICT auditing was being undertaken by either the internal audit departments or by external auditors. Most international and foreign owned banks exhibited thorough and in-depth ICT audit practices mainly being done by their company group audit teams with high level of specialization and sophistication as compared to the locally owned and the privately owned banks. All banks interviewed showed evidence of some level of ICT auditing processes that focused on the confidentiality, integrity and availability aspects of their ICT based systems. There was consensus in most cases in the areas of frequency of ICT audits and on key aspects that relate to the overall business continuity planning.

In addition to this, the field of ICT auditing and assurance is still relatively new and an emerging phenomenon in Kenya. Lack of adequate ICT audit guidelines and a compliance framework for Kenya was found to be a challenge to successful ICT auditing. In view of the complexity of the exercise, ICT is very technical and adequate evaluation of the state of the systems require specialized skills which in most cases are not readily available among the conventional audit teams. The support of the managements for ICT auditing was found to be critical for most of the challenges to be overcome.

In view of the above and in summary, this study gave a general view of the state of ICT auditing in commercial banks in Kenya by outlining the extent of ICT auditing and the major challenges that banks face in their effort to successful ICT auditing. The greatest beneficiary of this study is the society itself which will be able to enjoy greater confidence in information systems if all firms uphold and successfully practice objective ICT auditing.

5.3 Limitations of the study

A few limitations were encountered while undertaking this study. Some of the respondents and mainly from the privately owned banks were reluctant to disclose information relating to the topic and as a result the number of completed questionnaires was reduced. The target respondents were IT managers and some could not provide information regarding to the size in terms of staffing and number of accounts which were necessary to determine the size of the bank.

5.4 Recommendation for further research

A case study on ICT auditing may be required specific to any of the three main commercial banks: Standard Chartered, Barclays Bank or Kenya Commercial bank to get an in-depth understanding of the topic. The findings may be supplemented by interviewing the various ICT auditors in the internal audit department or from the major audit firms and consultants.

REFERENCES

Anderson, U., **"Assurance and Consulting Services,"** ***Research Opportunities in Internal Auditing,*** edited by A.D. Bailey, A.A. Gramling, and S. Ramamoorti (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2003).

AuditNet. www.auditnet.org

Audit procedures committee of AICPA, **Auditing standards and guidelines,** 1998

Barker, D., **Fighting Computer Crime**, Wiley Publications, 1998

Bower J. B.Et al, 18971: **Financial information systems**: Theory and practice. Allyn and Bacon publishers Boston

Callegos Fredrick, 1987: **Audit and control of information systems**, Smith Western publishing company

Carnegie Mellon University, **Capability Maturity Model Framework**.

Chambers, A. D 1990 **Computer Auditing** 3d Edition, Commerce learning House, IC

Chaplan. J., **Auditing Information Systems,** Wiley Publications, 1998 ",. 6. Dayton, D., *IT Audit Handbook,* Prentice Hall, 1997.

Collis, D. J and Montgomery, C. A (1995); **'Competing on Resources'** Published Paper, Harvard Business Review, September - October, 1995.

Computer Security Institute, **Eighth Annual CSI/FBI Computer Crime and Security Survey.** 2003., from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

Cuaresma, J.C., **"The Gramm-Leach-Bliley Act,"** *Berkeley Technology Law Journal* (17), 2002, pp. 497

Daveport T. H Hammer M., March –April 1989, **"How executive can shape their company's information systems"** Harvard Business Review, No.2

Dillard, J.F., and K. Yuthas, **"Ethics Research in AIS,"** *Researching Accounting as an Information Systems Discipline* edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Doyle, S., **"Advanced Information Technology"**, 1997

Efraim, T.,**"Electronic Commerce - A Managerial Perspective"**, Prentice Hall, 2002.

The Financial Sector Reform and Strengthening (FIRST) Initiative, 2006 http://www.firstinitiative.org/InformationExchange/Countries/country_information.cfm?iEligibleCountryID=70

Friedlob, G.T., F.J. Plewa, L.L.F. Schleifer, and C.D. Schou, "**An Auditor's Guide to Encryption (Altamonte Springs, FL"**, The Institute of Internal Auditors Research Foundation, 1997).

General Accounting Office (US), **"Federal Information Systems Controls Audit Manual"**, *GAO, 1999.*

Gatune J: **"Factors considered important in implementing local area networks:"** unpublished MBA Project, UoN July 1993.

Hargraves, K., S.B. Lione, K.L. Shackelford, and P.C. Tilton, *Privacy:* "**Assessing the Risk (Altamonte Springs, FL"**, The Institute of Internal Auditors Research Foundation, 2003).

Hickman, J. R., "**Practical IT Auditing**", Warren, Gorham and Lamont, 2000.

Huber, N., **"Business Scandals Put IT on the Spot,"** *Computer Weekly*, September 2002, p. 16

Hunton, J.E., "**The Participation of Accountants in All Aspects of AIS,"** *Researching Accounting as an Information Systems Discipline*, edited by V. Arnold and S.G. Sutton (Sarasota, FL: American Accounting Association Information Systems Section, 2002).

Information Systems Audit and Control Association (ISACA), CobiT: "**Control Objectives for Information and Related Technology, 3rd Edition"**, www.Isaca.org

Institute of Internal Auditors (IIA), http://www.theiia.org/itaudit/

International Federation of Accountants (IFAC), **"Auditing Standards"**, 2001 http://www.ifac.org/IAASB

Institute of Internal Auditors (IIA), **"Percent Audit Staff IT/IS Auditors – All Insurance Companies", (**2000, http://www.gain2.org/itis.html).

IsecT institute: http://www.isect.com/html/auditing.html

IT Web: http://www.itweb.co.za/sections/business/2006Audit.html

King, C.G., **"Protecting Online Privacy,"** *The CPA Journal*, November 2001, pp. 66-67.

Lainhart, J et al, **Computerised Information Systems Audit Manual**, ISACF, 1992.

Le Grand, C., **Information Technology in Auditing (Altamonte Springs, FL:** The Institute of Internal Auditors Research Foundation, 2001).

Makau, J. (1997); **'How Safe is the Web?'** PC World East Africa, June 1997.

Mbote, J. "**Influence of IT on Marketing:** The Case of Commercial Banks in Kenya", Unpublished MBA Thesis, University of Nairobi, 2003.

Ministry of Information & Communication: http://www.information.go.ke/policy/TPSP.pdf

Ndulu J.K. "**A survey of the causes of IS failure among microfinance institutions in Kenya**". Unpublished MBA Thesis, University of Nairobi, 2004.

Nyambane Thomas O. "**An evaluation of the extent of and factors limiting (IT) Usage in public quoted companies in Kenya**". Unpublished MBA Thesis, University of Nairobi, 1996.

Parker. X.L., *An e-Risk Primer* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2001).

Pressman. K., "**Software Engineering - A Practitioner's Approach**", Mc-Graw Hill, 2002

Reppel & Partners Pte, "**ICT Audit White Paper**", 2004.

RMIT University http://www.rmit.edu.au/

Rosenoer. J., D. Armstrong, and J.R. Gates, **Clickable Corporation: Successful Strategies for Capturing the Internet Advantage** (New York, NY: Arthur Andersen LLP, 1999).

Standard Chartered bank, "Group ICT Audit report", 2003

Warren, D. et al, **Handbook of IT Auditing**, Warren, Gorham and Lamont, 2001.

Weber. R., **Information Systems Controls and Audit,** Prentice Hall, 1999.

ANNEX I: ICT AUDIT QUESTIONNAIRE

Section A: Demographic factors

1. Year of incorporation of the bank ______________

2. What is the ownership structure of the bank? (Tick as appropriate)

   Public shareholding [ ]
   Privately owned [ ]
   Government owned [ ]

3. State the ownership of the bank______________? (Tick as appropriate)

   Local [ ]
   Foreign [ ]
   Partly local and partly foreign[✓]

4. Approximate number of employees in the bank ______________

5. Geographical coverage of the Bank's operations (Tick as appropriate)

   Local (within Kenya) [ ]
   Regional (East African Region) [ ]
   International (World wide) [ ]
   Other (specify)______________________

6. What is the bank's planning period? (Tick as appropriate)

   Quarterly [ ]
   Annualy [ ]
   Biannual [ ]
   5 years plan [ ]
   Others (specify) __________________

7. What is the bank's approximate number of account holders? (bank accounts) ______________

8. Does the bank have a fully-fledged ICT department? (Tick as appropriate)

Yes [ ] No [ ]

If "NO" to the above, under what department does ICT fall? ____________________

9. How extensive is the bank's Network?

Within Nairobi only [ ]

Extends country-wide [ ]

Regional (East Africa) [ ]

Within Africa [ ]

Others (specify) ______________________

10. Which of the following are computerized in the bank? (tick all those that apply)

Human resources management [ ]

Finance and accounting [ ]

Operations management [ ]

Marketing management [ ]

Customer services management [ ]

Other functions (specify) ______________________________

____

11. Does the bank use any locally developed computer applications (bespoke)?

Yes [ ]

No [ ]

12. How does the bank provide connectivity between its branches?

Public networks [ ]

Private network [ ]

Others (specify) __________________________

13. What ICT systems does the bank have? (Tick all those that apply)

Telecommunication systems VSAT, PABX, Routers etc [ ]
Communication and Collaboration Systems (e-Mail, Internet Site etc) [ ]
Financial System and accounting systems ---------------------------------- [ ]
E-banking systems -- [ ]
Customer Database systems --- [ ]
Workflow systems --- [ ]
Others (Please specify) ______________________________ [ ]
______________________________ [ ]

14. Are the ICT systems in the bank integrated or linked with each other?

Yes [ ] No [ ]

15. Are any of the bank's ICT systems integrated or linked with those of its customers?

Yes [ ] No [ ]

16. Are any of the bank's ICT systems integrated or linked with those of its service providers?

Yes [ ] No [ ]

17. Does the bank outsource any of its ICT systems or services?

Yes [ ] No [ ]

18. Is there an Internal Audit Department in the bank?

Yes [ ] No [ ]

19. If yes to (18) above, what is the size (number of staff) in the internal audit department? ____________________

Section B: Extent of ICT Auditing

To what extent does the bank's ICT Audit focus on the following? (Mark on a scale of 1 – 5)

5 - Greatest extent

4 - Great extent

3 - Moderate extent

2 - Less extent

1 - No extent

	1	**2**	**3**	**4**	**5**
Logical Security					
Configuration Management					
Systems Administration Procedures					
Hardware Inventory Management					
Software Licensing Compliance					
Data Backup					
Disaster Recovery Procedures					
Documentation					
Performance planning					
Capacity Planning					
Change Management					
Project Control					
ICT Strategy					
Controls – authorization, segregation					
ICT Security: passwords, Anti-virus software					
Service Level Agreements					
Firewalls configurations					
System downtimes					
Procedures					
Software licenses					
Electrical power, grounding systems					
Others (Specify)……………………..					
……………………………………					

3 Which of the categories of ICT applications are audited in the bank? (tick where all that apply)

Accounting system [ ]

Financial management system [ ]

Inventory/ stock management [ ]

Decision support system [ ]

Payroll systems [ ]

Sales and Marketing [ ]

Operations management systems [ ]

Human resources management systems [ ]

Others (specify) ______________________________

3. Who conducts ICT audit in the bank? (Tick as appropriate)

Internal Audit Department [ ]

External IT consultants [ ]

Audit firms [ ]

Company Group Audit team [ ]

Others (specify) _________________________

4. Where do the ICT auditors of the bank refer from for authoritative auditing guidelines for computerized systems?

Company guidelines [ ]

Local Auditing guidelines [ ]

International auditing guidelines [ ]

Others (specify) _________________________

5. To what extent does the bank's ICT Audit focus on the following? (Mark on a scale of 1 – 5)

Key:

5 – Greatest extent

4 - Great extent

3 – Moderate extent

2 - Less extent

1 - No extent

	1	2	3	4	5
Availability of services					
Disaster recovery					
Environmental controls					
Hardware maintenance					
Input and output controls					
Insurance of software and hardware					
Organizational controls					
Programming controls					
Resources planning					
Security controls					
Standards maintenance					
Risk management					
Physical access controls					
Staffing					
Regulation compliance					
Licensing					
Others (specify)					

6. Is ICT audit part of the financial audit of the bank?

Yes [ ]
No [ ]

7. How often does the bank carry out ICT audits (Tick as appropriate)

Once a year [ ]
Twice a year [ ]
Continuously [ ]
Ad-hoc [ ]
Never [ ]
Other (specify) ____________________

8. How is the Auditing of Information systems undertaken in the bank? (tick as appropriate)

Verifies accuracy of input and output only [ ]
Verifies accuracy and evaluates the computer programs [ ]
Uses Audit trails tracing a transaction through all stages [ ]
Uses CAATs (Computer Aided Audit Tools and Techniques [ ]

9. Which of the below best explains the scope of ICT audits in the bank? (Tick as appropriate)

Broadly-scoped with a wide range of aspects being generally reviewed [ ]
Narrowly-scoped with Higher Depth (detailed and very specific area) [ ]
A good mix between broadly-scoped and narrowly scoped [ ]

10. What reports are provided after the ICT audit in the bank?

Technical reports [ ]
Management reports [ ]
Both of the above [ ]

SECTION C: Challenges facing ICT Auditing in Bank

1 To what extent have the following been a challenge to the bank having successful ICT audits? (Mark in a scale of 1-5)

5 – Most challenging

4 - Challenging

3 – Fairly challenging

2 – Least challenging

1 – Not challenging

	1	2	3	4	5
Few numbers of users with computerized system					
Lack of trained and qualified staff					
Complexity of exercise					
Lack of cooperation from internal departments					
High training cost					
High cost of acquisition of computers and associated software					
Lack of ICT audit guidelines					
Challenges of coping with technology changes					
Lack of management appreciation of the importance of ICT auditing					
Budget constraints					
Poor assessments of threats and vulnerabilities					
Lack of awareness about ICT auditing					
Interpretation of ICT audit findings by senior managers					
Challenges of complexity of ICT infrastructure					
Poorly defined compliance framework (standards, copyrights)					
Lack of standard ICT audit framework/guidelines					
ICT Culture that ICT systems will always work well					
Conflict of interest					
Lack independence of auditors as they perform ICT audits					

To what extent have the following been a challenge to the bank having successful ICT audits?(Mark in a scale of 1-5)

5 – Most challenging

4 - Challenging

3 – Fairly challenging

2 – Least challenging

1 – Not challenging

	1	**2**	**3**	**4**	**5**
Time constraints					
Destruction of ICT audit trails by the auditee					
Problem of ICT audit Scope definition					
Unavailability of data required by the ICT auditor					
Lack of ICT auditing skills					
Difficulties in identification of ICT risks					
Limited management support and commitment					
The interdependency of customers' and suppliers' processing and outsourcing of ICT services					
Poor usage of Computer Aided Audit Tools in ICT auditing					
Translation of ICT audit findings into business impacts that managers can relate					
Translation of ICT audit findings into vulnerabilities that managers can relate					
Others (specify)					

ANNEX II: LIST OF COMMERCIAL BANKS IN KENYA

1. African Banking Corporation, Nairobi
2. Akiba Bank, Nairobi
3. Bank of Africa
4. Bank of Baroda, Nairobi
5. Bank of India, Nairobi
6. Barclays Bank of Kenya, Nairobi
7. CFC Bank, Nairobi
8. Charterhouse Bank Ltd, Nairobi
9. Chase Bank Ltd, Nairobi
10. Citibank, Nairobi
11. City Finance Bank, Nairobi
12. Co-operative Bank of Kenya, Nairobi
13. Commercial Bank of Africa, Nairobi
14. Consolidated Bank of Kenya Ltd, Nairobi
15. Credit Agricole Indosuez, Nairobi
16. Credit Bank Ltd, Nairobi
17. Delphis Bank, Nairobi
18. Development Bank of Kenya, Nairobi
19. Diamond Trust Bank, Nairobi
20. Dubai Bank Kenya Ltd, Nairobi
21. Equatorial Commercial Bank Ltd, Nairobi
22. Fidelity Commercial Bank Ltd, Nairobi
23. Fina Bank Ltd, Nairobi

24. First American Bank of Kenya, Nairobi

25. Giro Commercial Bank Ltd, Nairobi

26. Guardian Bank, Nairobi

27. Habib Bank A.G. Zurich, Nairobi

28. Habib Bank Ltd, Nairobi

29. Housing Finance Co. Ltd, Nairobi

30. Imperial Bank, Nairobi

31. Industrial Development Bank, Nairobi

32. Investment & Mortgages Bank Ltd, Nairobi

33. K-Rep Bank Ltd, Nairobi

34. Kenya Commercial Bank Ltd, Nairobi

35. Middle East Bank, Nairobi

36. National Bank of Kenya, Nairobi

37. National Industrial Credit Bank Ltd, Nairobi

38. Oriental Commercial Bank Ltd, Nairobi

39. Paramount Universal Bank Ltd, Nairobi

40. Prime Bank Ltd, Nairobi

41. Prime Capital and Credit Ltd, Nairobi

42. Southern Credit Banking Corp. Ltd, Nairobi

43. Stanbic Bank Kenya Ltd, Nairobi

44. Standard Chartered Bank , Nairobi

45. Trans-National Bank Ltd, Nairobi

46. Victoria Commercial Bank Ltd, Nairobi