KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY,

KUMASI

COLLEGE OF SCIENCE

INSTITUTE OF DISTANCE LEARNING

INVESTIGATING THE EFFECTIVENESS OF INFORMATION TECHNOLOGY AUDIT CONTROLS IN FINANCIAL INSTITUTIONS

(A CASE STUDY OF SIXTEEN RURAL BANKS IN GHANA)

BY

ABAIDOO EMMANUEL KWAME

(BSC. COMPUTER SCIENCE)

(PG 6552611)

NOVEMBER, 2015

INVESTIGATING THE EFFECTIVENESS OF INFORMATION TECHNOLOGY AUDIT CONTROLS IN FINANCIAL INSTITUTIONS (A CASE STUDY OF SIXTEEN RURAL BANKS IN GHANA)

KNUST

BY

ABAIDOO EMMANUEL KWAME

(BSC. COMPUTER SCIENCE)

(PG 6552611)

A Thesis submitted to the Computer Science Department, Kwame Nkrumah University and Science and Technology in partial fulfillment of the requirement of the degree

Of

MASTER OF SCIENCE INFORMATION TECHNOLOGY

NOVEMBER, 2015

DECLARATION

I hereby declare that this submission is my own work towards the MSc Information Technology (MSc Info Tech.) degree and that, to the best of my knowledge, it contains no material previously published by another person nor material which has been accepted for the award of any other degree of the university, except where due acknowledgement has been made in the text.

KNUST

Abaidoo Emmanuel Kwame ……..…… ……..……

(PG 6552611) Signature Date

Certified by:

Mr. I.J. Arthur ……..…… ……..……

(Supervisor) Signature Date

Certified by:

Dr. J. B. Hayfron-Acquah ……..…… ……..……

(Head, Computer Science Dept, KNUST) Signature Date

ABSTRACT

Investigating the effectiveness of information technology (IT) Audit controls in financial institutions was worth researching, regarding the increasing number of financial

institutions resorting to computerization. Thus, these institutions would primarily depend on IT audit controls that are put in place to manage and guard the institutions' overall business setup to achieve the institutions' business goals or objectives. The main objectives of the research were to find out the kind of IT Audit Controls being used, Controls' weakness, its causes and effects and the recommendations needed to ensure controls' effectiveness. Sixteen computerized financial institutions were sampled and the IT Controls used were studied. In spite of the successes made by the computerized financial institutions, the sampled financial institutions helplessly admitted to the dangers posed by other IT security challenges. These IT security challenges were mainly as a result of internal control weakness which potentially can bring the institutions down if not checked. Considering the globalization of the computerized technology it was recommended that the financial institutions in the country should employ more of these IT Audit controls, especially Internet and ECommerce Controls, Telecommunication Controls and Database Controls in the dayto-day transactions. Also for optimum effectiveness of these Controls, the computerized financial institutions should also pay every price to strengthen the internal controls to safeguard against avoidable IT Audit controls' breaches and other potential security challenges that can break down the financial institutions. Further research must be undertaken to investigate the recent spate of global banking fraud on credit and debit cards of customers who patronize electronic commerce.

DEDICATION

I dedicate this work to God, my Creator and my family.

ACKNOWLEDGEMENT

I profoundly acknowledge God's provision for this great accomplishment. I wish to thank all the Computer Science Department lecturers for their respective encouragement. I am highly indebted to my supervisor Mr. I. J. Arthur for his time, contribution, encouragement, suggestion, persistent calls and direction in spite of his busy schedules.

I also wish to express my profound appreciation to Mr. Frimpong Twum for his time and invaluable contribution to this great achievement. My deepest gratitude goes to my wife and children for their patience for this feat. To Mr. and Mrs. Adafia of ICGCKumasi, I acknowledge your indelible contribution to this attainment. I wish to also express my sincere thanks to the staff of all the sampled computerized financial institutions who contributed greatly to this success.

My final gratitude goes to Professor R. C. Abaidoo and wife who also persistently prevailed over me to accomplish this research work. To all of you who in diverse ways made this work a reality, I say thank you. May God richly bless you all.

TABLE OF CONTENTS

KNUST

KNUST

LIST OF TABLES

 LIST OF FIGURES

KNUST

CHAPTER ONE

INTRODUCTION

1.0 Background to the Study

The idea of Information Technology (IT) Audit which has been in existence since the mid-1960s has metamorphically undergone various stages, mainly due to unfolding discoveries made in the technology and the integration of the technology into businesses (Rainer et al., 2011).

Currently there are a lot of companies that rely on the Information Technology (IT) for their day-to-day operations; among such are Telecommunication companies, Banking institutions and many others. For these organizations, IT plays big part of their day-today activities including the employment of setup systems that are more dependable to enhance the institutions' activities and operations. The above, thus underscores the fact that the application of IT in organizations, institutions, companies, enterprises and the like is constantly increasing.

Information Technology (IT) Audit which is also known as Information Systems (IS) Audit is the evaluation of organizations' daily transactions, activities, procedures, operations or setups within an Information System infrastructure (Rainer et al., 2011). Thus the primary function of an IT audit is to electronically examine to find out the institutions' capability to use Information Technology infrastructure to secure its hard earned valuables or assets and also communicate and disseminate information to appropriate people. In financial institutions these reviews are done to evaluate whether IT based financial organizations are adhering to standard accounting practices.

Information Technology (IT) Audits are usually performed by IT Audit professionals with professional certification from international organizations such as Institute of Internal

Auditors (IIA), Certified Information System Auditor (CISA), just to mention a few (Rainer et al., 2011).

1.1 Audit Controls

Audit Controls are usually institutions' setups, mechanisms, frameworks and organizational structures which are used for the inspection of the accounting procedures and records by a trained auditor to eliminate or minimize dangers or losses to the organization. The Audit controls seek to address two main objectives, such as achieving the institutions' goal and risks or losses which must be prevented (Kenneth, 2010).

"Without audit, no accountability; without accountability, no controls; without controls, no efficiency; without efficiency, no development" (Daniel, 1999). This emphasizes the importance of audit in every organization.

1.2 Information Technology (IT) Audit Controls

These are distinctive setups and procedures that are electronically defined by institutions to effectively and efficiently bring to pass the realization of the institutions' objectives and set goals. The objectives of these distinctive setups and procedures also focus on sensitivity, wholeness, and accessibility of data and the entire management of the information technology setup, (PCAOB, 2007).

According to PROTIVITI (2009), these procedures and setups usually include the following:

i. Security and right to organizations' information and systems controls, ii. Setups relating to the administration of the organizations' business and its operations,

iii. Procedures for triggers, iv. Procedures that identify and manage the organizations valuables,

v. Setups that ensure continuity of business operations, vi. Storage and retrieval support systems, vii. Systems that ensure proper management and storage of data or information, viii. Systems that monitor and manage the transmission of organizations' information, ix. Systems that address the dangers and risks to confidential and crucial organizations' information, et cetera.

These distinctive setups and procedures or controls above are used to monitor, manage and ensure that the organizations physical assets, information assets, its surroundings, the workforce, operations and customers are protected and secured.

1.2.1 System Log Files

The system log file contains is also security support system that contains records or evidence of various daily transactions of the organization as tracked by computer systems. Such tracked records provide vital information such as when a computer user uses the computer to transact business, problems encountered by the computer systems, et cetera, (Bonsor, 2001). These recorded transactions are specifically by the operating systems being run on the computer system and can be checked by the event viewer, (Microsoft, 2012).

1.2.16 Audit Trail

Also a security support system that shows proofs or footprints of all electronic transactions that one or a user uses the computer system to transact. This security support system is part and parcel of most accounting and database programs, (Vangie, 2014).

1.3 Information Technology (IT) Auditors and What They Do

According to Rainer et al. (2011) Information Technology Auditors mainly study and ascertain the effectiveness of technical and procedural setups of organizations' systems

to counteract anticipated and avoidable risks. The IT Auditors evaluate risks relating to IT systems and processes including the following as a framework:

i. Inadequate information security (e.g. security control systems breaches, missing or out of date antivirus controls). ii. IT related frauds (investigating perceived frauds).

iii. Verification of the security procedures. iv. To check procedures for system management.

v. To verify the existence of control mechanism over vendor access. vi. Obtain and review the various report from the systems in place, vii. Review the overall supervision by management over system activities.

viii. Inefficient use of corporate resources, or poor governance.

In addition, the IT Auditors, in various fields of discipline engage themselves in all kinds of audit such as:

i. Client/Server, Telecommunications, Intranets, and Extranets audit

ii. Management of IT and Enterprise Architecture audit iii. ICT Installation Audits iv. Operational Computer System And Network Audits

v. Information Security Audit vi. ICT Strategic Audit

vii. Change Management Audit viii. ICT Disaster Recovery Audits, etc.

However, the scope of the research has been carefully chosen to guide the research work as indicated below.

1.4 Problem Statement

This section briefly talks about the inherent problems that the stakeholders of the above have to confront with, which primarily focuses the attention of the problem solving team. IT Auditors of institutions however, have to brace themselves up against some IT security breaches or challenges which could be very threatening to the very existence of the technology.

IT security controls' threat is anything that unlawfully tries to gains access to any IT security infrastructure which in turn makes non effect the underlying security controls or mechanisms (controls, policies, practices or procedures) of the IT infrastructure system. This unlawful acts result in an unauthorized access to data, applications, services, computer networks and/or devices (BusinessDictionary.com, 2014). These breaches or challenges have been a major menace, especially to computerized financial institutions globally. Hence, there are a number of international industrial guidelines and government compliance regulations mandate worldwide for strict governance of sensitive data for possible avoidance of information breaches or threats (Margaret, 2010).

Thus, there are no breaches free IT security controls even at the international levels. Collaboratively such breaches or threats however, can be controlled internationally if internal security controls are adhered to and are properly and strictly managed globally. It thus behooves all stakeholders of the above, especially IT based financial institutions to relentlessly battle these controls' breaches out to objectively enable them achieve the organizations' business goals.

1.5 Research Objectives The

main objectives are:

i. To find out the kind of IT Audit Controls being used in financial institutions.

ii. To find out possible breaches or threats in these Controls iii. To determine the causes and effects of such Controls' breaches.

iv. To recommend way(s) of possibly eliminating or reducing to the barest minimum such breaches to ensure effectiveness in IT Audit Controls.

KNUST

1.6 Research Questions

These are:

i. What kind of IT Audit Controls are being used? ii. What are the possible breaches in these Controls? iii. What are the causes and effects of such IT Audit Controls' breaches? iv. What recommendation can be made to possibly eliminate or reduce to the barest minimum such IT Audit Control Systems' breaches to ensure effectiveness?

1.7 Significance of the Study

Needless to say, the research work may not have any material reward for the researcher but it is of intellectual interest to the researcher. The research findings would also add up to the researcher's academicism. Again, the research work, to a large extent, will also help identify challenges encountered by financial institutions that employ the computerized technology for their daily transactions, and also help recommend solutions or effective ways to overcome such challenges. Furthermore, findings of the study would be beneficial to many stakeholders who are already using the technology, and also others who are contemplating employing the technology but are not certain of the technology's value for money.

Eventually, the research findings would enable financial institutions especially, management and shareholders of the institutions to:

i. Electronically discover what goes on or happens at any point in time; ii. Take precautionary steps to address possible danger before they become too late to be fixed; iii. Objectively examine and ascertain organizations' setups critically iv. Embrace realities and make well informed decisions;

v. Take necessary actions to carry out effective renovations where needed; vi. Eliminate corrupt practices where possible; and vii. Rely accurately on application and operations of IT in day-to-day work.

1.8 Justification of the study

This study therefore seeks to bring to light, if not all, some of the hidden practices of security controls' breaches or challenges in IT Audit, its related effects and what should be done effectively to possibly eliminate or reduce to the barest minimum such security breaches and its related frauds.

1.9 Research Methods (Strategy)

The researcher will make use of both qualitative and quantitative techniques to gather all data necessary for the research. In this study, data will be gathered qualitatively using interviews, questionnaires and observations from the selected computerized banking institutions, followed by quantitative analysis.

Data for the study will be derived from sixteen (16) computerized financial institutions and this will be the primary source of data. With regards to this primary source of data that will be used in this research work, information will be gathered from rural banks. More emphasis is placed on the primary data source because of its reliability and validity to the research work. The data collected will be analyzed using the Statistical Package for Social Scientists (SPSS) version 21.0 and Microsoft excel.

The study will be concentrated primarily in three major regions of Ghana, thus Ashanti, Central and Western regions. The findings of this research derived from these noncommercial computerized banks from the three chosen regions can be inferred nationally.

1.10 Scope and Limitations

Several constraints are anticipated. The major one will be difficulties in data collection, since all the targeted financial institutions for the primary source of data deal with highly sensitive data. Also the need to self-administer questionnaires and collect all the administered questionnaires on the spot is a major source of worry since respondents cannot be trusted to guarantee the safety of the questionnaires. Also, no auditing software tool will be used. The designed questionnaires, interviews and observations will be the research instruments.

Again, other constraint has to do with the topic under investigation, the researcher, for lack of time and financial resources carefully limited the research to cover security controls that underpin the following areas of IT Audits Rainer et al. (2011):

i. Inadequate information security (e.g. security control systems breaches, missing or out of date antivirus controls).

ii. IT related frauds (investigating perceived frauds).

iii. Verification of the security procedures. iv. To check procedures for system management.

v. To verify the existence of controls' mechanisms over vendor access. vi. System activity reports.

vii. Review the overall supervision by management over system activities viii. Ineffective IT strategies, policies and practices, etc.

Furthermore, the research work as stated above is focused on IT based financial institutions (computerized rural banks) in Ghana. However, the researcher with limited time and financial resources, and for easy access of information, has again carefully chosen the following computerized banking institutions from the three regions (Ashanti, Central and Western) of Ghana for the case study. Nevertheless, the limitations above would not prevent institutions with similar characteristics to benefit from the findings of this research.

The sampled financial institutions are as follows:

i. Adansi Rural Bank Ltd., Fomena-Ashanti Region ii. Amansie West Rural Bank Ltd., Antoakrom-Ashanti Region iii. Asokore Rural Bank Ltd., Asokore-Ashanti Region iv. Atwima Kwanwoma Rural Bank Ltd., Foase. -Ashanti Region

v. Bosomtwe Rural Bank Ltd., Kuntanase-Ashanti Region vi. Juaben Rural Bank Ltd., Juaben-Ashanti Region vii. Nsutaman Rural Bank Ltd. , Nsuta-Ashanti Region viii. Kwamanman Rural Bank Ltd. , Bomso-Ashanti Region ix. Mfanseman Commercial Bank Ltd. , Biriwa-Central Region

x. Assiman Rural Bank Ltd., Assin Manso-Central Region

xi. Kakum Rural Bank Ltd, Elmina-Central Region xii. Akatakyiman Rural Bank Ltd. , Komenda-Central Region xiii. Ahantaman Rural Bank Ltd., Agona Nkwanta-Western Region xiv. Amenfiman Rural Bank Ltd., Wassa Akropong-Western Region xv. Lower Pra Rural Bank Ltd., Shama-Western Region xvi. Western Rural Bank Ltd., Sekondi-Western Region

1.11 Thesis Organization

This research is organized into five chapters with Chapter One covering the background information, statement of problem, objectives of the study, research question, significance of the study, justification of the study, methodology, scope of the study, limitations and organization of the report. Chapter two covers the review of related literature on investigating the effectiveness of IT audit Controls in financial institutions. Chapter three also explains the research methodology, the profile of selected banking institutions of the research and the frame work for IT Audit access authorization controls in rural banks. Chapter four covers the analysis of results and discussions. The last chapter, Chapter five concludes, summarizes findings and recommendations of IT Audit controls and the suggested future work.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter discusses some of the available literature reviews on the effectiveness of IT Audit controls. It also looks at summary of abstracts on various literatures with regard to the model being used and the general working title. The Chapter comprises both theoretical literature and empirical literature

2.1 Theoretical literature

This section of the study presents literature relating to the subject matter based on definitions and discussions of some terminologies in the aspect of Information Technology audit, audit controls among others.

2.2 Information Technology Audit

Information Technology (IT) Audit which is also known as Information Systems (IS)

Audit is the evaluation of organizations' daily transactions, activities, procedures, operations or setups within an Information System infrastructure, (Rainer et al., 2011). Thus the primary function of an IT audit is to electronically examine to find out the institutions' capability to use Information Technology infrastructure to secure its hard earned valuables or assets and also communicate and disseminate information to appropriate people. In financial institutions these reviews are done to evaluate whether IT based financial organizations are adhering to standard accounting practices.

For an institution to bring to pass its objectives and stated goals, an effective IT infrastructure should be maintained, (Rainer et al., 2011).

Levine (2013) in her report on proposed IT audit scope to support annual statement audit, indicated that IT Audit needs to instill confidence in IT setups relating to data completeness are capable of producing intended results for annual statements.

2.2.1 Types of Information Technology Audit Controls

According to Rainer et al. (2011), the various IT Audit controls can be categorized into three. These are:

i. Setups and procedures that are intended to offer security and advanced remedies to systems.

ii. Setups and procedures readily available to perceive the existence of any act that contravenes the systems and iii. Setups and procedures in readiness to react to events and situations contravening the systems rather than instigating against them.

2.2.2 Significance of Controls

According to INTOSAI, (2014), the importance of setups and procedures in computer systems cannot be overemphasized. These controls invariably guide against:

i. Loss of information when files are damaged, ii. Adulteration of data, iii. Fire outbreaks, power failures and illegal entry into systems, iv. Virus attacks on system et cetera.

2.2.3 The Role of Information Technology Audit

Assessing the dependability, wholeness and completeness of the organizations' IT setups and procedures is the main objective of the organizations' internal IT audit. This assessment invariably helps to keep in checks, the continued existence, the competency and result oriented procedures and setups of the organizations, (Goldberg, 2011).

2.3 Audit Controls

Audit Controls are usually institutions' setups, mechanisms, frameworks and organizational structures which are used for the inspection of the accounting procedures and records by a trained auditor to eliminate or minimize dangers or losses to the organization. The Audit controls seek to address two main objectives, such as achieving the institutions' goal and risks or losses which must be prevented, (Kenneth, 2010).

These are distinctive setups and procedures that are electronically defined by institutions to effectively and efficiently bring to pass the realization of the institutions' objectives and set goals. The objectives of these distinctive setups and procedures also focus on sensitivity, wholeness, and accessibility of data and the entire management of the information technology setup, (PCAOB, 2007).

According to PROTIVITI (2009), these procedures and setups usually include the following:

i. Security and right to organizations' information and systems controls, ii. Setups relating to the administration of the organizations' business and its operations, iii.

Procedures for triggers, iv. Procedures that identify and manage the organizations valuables,

v. Setups that ensure continuity of business operations, vi. Storage and retrieval support systems, vii. Systems that ensure proper management and storage of data or information, viii. Systems that monitor and manage the transmission of organizations' information, ix. Systems that address the dangers and risks to confidential and crucial organizations' information, et cetera.

These distinctive setups and procedures or controls above are used to monitor, manage and ensure that the organizations physical assets, information assets, its surroundings, the workforce, operations and customers are protected and secured.

Al-Twaijry et al. (2004) indicated that, the result oriented internal control systems of any organization help others to rely on the work of internal auditors and thereby enhancing the systems' ability to achieve results.

According to Anantha (2002), a general examination of setups and procedures of an organization is an effort to have an insight or opinion of the various controls that are present in the organizations' business information systems.

2.3.1 Auditing Application controls

Anantha (2002), defined Application software as the software that handles, manages and monitors the institutions' proceedings. Application software setups and procedures relate to the ambit of individual organization procedures which include data modifications, assigned distinctive organization actions and activities, reconciliation of books, various system reports, et cetera.

In reviewing the application software, one considers questions such as, "What does the application software do; what business function it perform?" It is thus very important for the IS auditor to be familiar with organizations function that the application software is designed to fulfill. Another way to also achieve this feat is to conduct an interview involving the workforce. Afterwards, it is very imperative to also establish the likely dangers closely connected to the organizations' setups that the application software is designed to serve and also examine how these dangers are managed by the software, (Anantha, 2002).

2.3.2 Authorization and Authentication Controls

Authorization setups and procedures basically ensure that one is given the legal right to access the system. Authentication setups and procedures on the other hand evaluate users' logins to ensure that the logins belong to the designated users. In authorization and authentication setups and procedures it is very important for the organization to adopt prudent measures to ensure well defined procedures of sequence of characters that must be used or keyed in by the system users to gain access, (Singleton, 2008).

2.4.3 Determinants of Control Systems Strength

Ge et al. (2005) indicated that the strength, wholeness and completeness of internal setups and procedures invariably rely on organizations ability to manage and monitor its procedure, practices and policies overseeing its valuables, purchases, sales, account management and employee recruitment.

2.4.4 Common Weaknesses of Control Systems

Albrecht et al. (1984) put forward some weaknesses of internal setups and procedures as follows:

i. Having a lot of confidence in employed staff, ii. Improper setup and practices for password verification and validation, iii. Undeclared financial status of organization's personnel

iv. Inability to isolate business dealings from caretakers of organization's valuables,

v. Failure to have prudent checks on effectiveness and efficiency, vi. Inability to pay meticulous details to particulars, vii. Inability to isolate organization's valuables from valuable accountability, viii. Inability to have distinctive accountable obligations, ix. Failure to have distinctive lines of administrative controls,

x. Inability to systematically examine systems' reports, xi. Absence of requirements or conditions for conflicting interest and xii. Inadequate documentations and information

2.5 The Minimum IT Controls to Assess in a Financial Audit

In a part II of a Journal published by ISACA (2011), authored by Goldberg (2011), a framework outlined to guide IT auditors in financial auditing. The framework focuses on five basic areas of ITGC which are considered very essential for examination. These are:

i. IT Setups and procedures that govern the organization's surroundings

ii. Setups and procedures that focus on innovations iii. Setups and procedures that focus on data security iv. Setups and procedures that focus on support systems for data storage and data retrieval

v. Setups and procedures that focus on user support systems

2.6 Empirical Literature

This section chronicles summaries of reviews on research articles/papers, books, conference proceedings, magazines relating to the IT audit controls.

An experimental and analytical studies to investigate the adequacy of security controls, by Musa (2004), in the Egyptian Banking Industries (EBI) discovered that computer departments paid relatively more attention to IT security setup procedures that focus on computerized software being used rather than that of the organization. However, the internal audit departments focused more on security setup procedures relating to behavior and institution rather than that of the computerized software

Hayale and Khadra, (2006), researched into the topic "Evaluation of the effectiveness of controls in computerized accounting information systems: an empirical research applied on Jordanian banking sector". The main objective of the study was to examine and find out the extent of result-oriented setup procedures in Computerized Accounting Information Systems (CAIS) in order to maintain sensitivity, wholeness, exactness, completeness and accessibility of the bank's data. The study discovered that the Jordanian domestic banks focalized on result-oriented setups and procedures in combating frauds and minimizing system errors.

Pathak (2009) studied 'IT audit and electronic transfer systems'. The researcher aimed at providing a framework for evaluating the effectiveness of electronic mobile money transfers. The researcher concluded that for effective electronic money transfer systems internal auditors of organizations must have in place prudent internal setups and procedures to handle, manage and monitor electronic funds transfers to curb potential losses.

Badara and Saidin (2013) reviewed the relation that existed between 'result- oriented IT audit internal setup procedures and internal audit result-oriented at local government

level'. The conclusion was, the result-oriented IT audit internal setup procedures can directly determine the performance of internal auditors at the local government level.

Bruce (2014) wrote on the topic 'Full disclosure -- the practice of making the details of security vulnerabilities public'. In his write up he explained computer security to comprise security of information and valuables from theft, adulteration, or natural forces. He permitted information and valuables to be kept available and productive to its designated users. The researcher concluded that the abuse of computer hardware such as keyboards, screens, printers, network cards, memories and processors could lead to sensitive data loss.

ISACA (2014) cited Singleton (2008), the author of 'What Every IT Auditor Should Know About Auditing Information Security' as one who came out with assertion that there are three shortfalls that explain the popularity related to security awareness:

i. He asserted that most institutions are deficient in prudent setup procedures.
ii. The absences of illegal access setup procedures which are deficient in most institutions,
iii. A third deficiency from the researcher is the use of 'patches' for system susceptibility to attacks, (Singleton, 2008).

A recent article by REUTERS (2014), on 'Home Depot confirmed security breach following Target data theft'. Home Depot Inc., a computerized firm, confirmed on Monday, September 8, 2014 that the data theft confirmed a breach in payment systems' IT security controls. It was feared that this could have effect on its customers.

Adam (2013), the former director of the New Jersey Division of Consumer Affairs and chairman and co-founder of Credit.com, wrote on the topic: 'The Identity Theft Flu: 5 Ways to Keep Yourself Healthy'. The Article defined Identity theft as illegally using somebody's credentials or identities to engage in fraudulent deals electronically. He inferred that this unfortunate crime makes nonsense of all the IT security setups and procedures.

iREACH (2013), published an article on '2012 Sets New Record for Reported Data Breaches'. It was discovered that the identity theft assumed an alarming proportion in the previous year.

According to Adam (2013), hackers fraudulently and unauthorizedly accessed and made away with adequate personal information of famous personalities such as First Lady Michelle Obama, Vice President Joe Biden, Jay-Z, Beyonce and Secretary of State Hillary Clinton. According to Adam (2013) a lot of cash from ATM systems via prepaid debit cards were stolen in a matter of hours across the globe.

Zak (2014), the managing editor of Internet Retailer Magazine, wrote on the topic: 'The war with no end". He reported that criminals were relentlessly looking for loopholes in security setups of systems to break through. Thus the need for everybody to maintain a perfect defense electronically.

Eshel et al. (2014), wrote on the article 'A Changing Battle Space: Prevention Is Not Enough'. The writers admittedly asserted the claim that 'Surviving a shark attack is fairly simple: As long as you swim faster than the person next to you, chances are that you'll make it". They continued that the well-known IT security setups and procedures were no

longer adequate to hackers electronically. The writers affirmed that the modern day attacks are more pertinent and more convoluted than ever before.

Osborne (2014) wrote on the article 'Between The Lines' . In this article the writer categorically stated that the Federal Bureau of Investigation (FBI) has mercilessly set out to investigate the IT security breach or attack which made a considerable number of high-profile personalities fall victims.

KNUST

2.6 Summary Of Literature Review

From the theoretical and empirical literature reviews above, it is clear that the progress of every Nation invariably thrives on effective and efficient set of prudent internal controls adopted by the government and individuals in their daily operations. The success and sustenance of these controls also depend on the strength of these internal controls.

The above studies thus revealed that, for any computerized organization to bring home the bacon the institutions must put in place effective and efficient IT Audit controls. Thus, the success of computerized organizations, institutions and the like largely depend on the effective implementation of these controls.

Per the above studies, the computerized financial institutions do have some measure of effectiveness with IT audit controls, but there are still security challenges that come with the computerized technology. Unfortunately the tendencies of these security challenges or IT audit controls' breaches are that the affected institutions are always left unprotected and clueless to the sophistication of scammers, fraudsters and identity theft services.

In conclusion, the effectiveness of IT audit controls is dependent on the institutions ability to strengthen their internal controls' systems against any avoidable IT Audit controls' breaches and other potential security challenges.

CHAPTER THREE

RESEARCH METHODOLOGY

KNUST

3.0 Introduction

This chapter outlines the choice of study approach and strategy that was used in undertaking the study. It also gives account of how the study was conducted and states the main players that were used, including the statistical schemes used in analyzing collected data. Furthermore it also briefly touches on the profiles of all the sampled computerized financial institutions.

3.1 Research Design

According to Malhotra (2007), research design is the methodology for carrying out any research. It is the fundamental scheme for carrying out data collection and analysis phase or as "blueprint" for research. Research design also at least touches on what to do, which data to gather, and how to analyze the results (Robson, 2002). The main sampling technique was purposive sampling procedure. Purposive sampling is when the people selected are the key individuals who can give the information require for study. Questionnaire was designed for the bank staff (mainly tellers and other system users) to obtain information on IT Audit controls being employed by the institutions.

3.2 Research Process

The best process relies on the study questions and the predilection of the researcher. For this study, the research process first considered designing an interview guide to help the researcher gather information as to who plays what roles in the daily administration and

operations of the selected banks. Furthermore, the interview guide was used to find out the main work of the internal auditors, category of system users and types of IT Audit controls used and also to identify the respective respondents for the questionnaire to be developed in the computerized financial institutions. Interview was also used to gather the secondary data (source document) from the institutions. Secondly, the research also considered sixteen (16) computerized rural banks for the case study. Thirdly, the research design used questionnaires to focus on the IT audit controls involved in the following technical and procedural controls, as the main framework for the investigation, as outlined by Rainer et al. (2011):

i. Inadequate information security (e.g. security control systems breaches, missing or out of date antivirus controls) ii. IT related frauds (investigating perceived frauds) iii. Verification of the security procedures iv. To check procedures for system management

v. To verify the existence of control mechanism over vendor access vi.

Review of all various reports from the systems in place vii. Review the overall supervision by management over system activities viii.

Ineffective IT strategies, policies and practices, etc.

3.3 Research Assumptions

The research study assumed that the selected computerized rural Banks have been in existence for some time now and thus would appreciate the research work.

3.4 Study Population

Study population according to Bryman and Bell (2003), is the entire group that the study addresses. The research study population focuses on all computerized Rural Banks in Ghana.

3.4.1 Sampling Method/Design

The main sampling technique used was purposive procedure. Purposive sampling is when the people selected are the key individuals who can give the information require for the study. Questionnaires were designed for the selected banks. Each bank was served with questionnaires.

3.4.2 Sample Size

The study used a sample size of sixteen (16) computerized financial institutions (noncommercial banks). For each financial institution, the following constituted the questionnaires' respondents since they are responsible for the day-to-day administration and operations of the bank. They are the management team (the General Manager/Chief Executive Officer, Head of Accounts Department, Head of ICT Department, Head of Audit Department) System Administrators and the Tellers (Cashiers). This convenience sampling technique was employed since all computerized rural banks have common banking features, practices, policies and procedures.

3.5 Sources of Data

The data employed in this study are both primary and secondary. The primary data was collected through self-administered questionnaires, and secondary data was obtained from institutional documents and other system generated reports such as audit trails/report and log files using an interview guide.

3.5.1 Data Collection Instruments

The study used mainly questionnaires for data collection. The questionnaire designed was well structured for collecting primary data. Other instruments such as interviews and observations were also employed. An interview guide was thus developed for soliciting secondary data from management and other key respondents.

3.6 Method of Analysis

Simple descriptive statistics was applied in analyzing the data. Two statistical software packages called Statistical Package for Social Sciences (SPSS) and Microsoft Excel used for the analysis. Tables, percentages and bar charts were also employed in illustrating the results. Questionnaires administered were first edited and then values corresponding to respondents responses were converted to percentages for easy analysis.

KNUST

3.7 Profile of Association of Rural Banks (ARB)- Apex Bank Limited

The registered non-commercial banks in all the 10 regions in Ghana are about 135. (ARB, 2013). All of them fall under the umbrella of Association of Rural Banks-ARB Apex Bank Limited. The ARB Apex Bank Ltd provides the supervisory role for all registered rural banks in Ghana and beyond the borders of Ghana. Financing is mainly done through the Rural Financial Services Project (RFSP), a Government of Ghana project to collectively help tackle challenges the confront the banks. The vision of the ARB Apex Bank Ltd is to strategically provide a cutting-edge technology to optimize gratification of Rural and Community Banks (RCBs). The mission of the ARB Apex bank Ltd. is to make available viable banking and non-banking back up services to the RCBs with the objective of optimizing their functional performance and customer service, and eventually help financial institutions to bring home the bacon

3.7.1 Brief Profile of the Sampled Rural Banks

Needless to say, all the sixteen (16) sampled computerized rural banks for the case study are all affiliated to ARB Apex Bank Limited. The following are brief profiles of the sampled rural banks or financial institutions courtesy ARB, (2013).

- **Ahantaman Rural Bank Limited,** established in 1984 to do the business of Banking. Its headadquarters at Agona Nkwanta, in Western Region. The Bank

currently operates in four districts in the Western Region with a network of twelve connected Branches.

- **The Kumawuman Rural Bank Limited** is the sixth Rural Bank to be established in the Ashanti Region, and the 45th in Ghana. The Bank is now computerized and networked all its eleven branches.

- **Asokore Rural Bank Limited** has its headquarters at Asokore, in Ashanti Region. The Bank has now computerized and networked all its seven branches.

- **Atwima Kwanwoma Rural bank Limited** was established on the 6th of September 1983 as a financial institution empowered by the bank of Ghana. It was the 68th rural bank to be established in the country and the 13th rural bank in the Ashanti. It has computerized all its seven branches.

- **Bosomtwe Rural Bank Limited** was incorporated in Ghana in November 1981, and it was authorized to carry on the business of banking under the Banking Act, 1970 (Act 339) on 9th December 1982. Its headquarters is at Kuntanase in the Ashanti Region. It has nine branches and has computerized all branches.

- **Juaben Rural bank Limited,** also was incorporated on 24th October, 1984, as a Rural Bank and has since then built a reputation as one of the leading Rural banks in Ghana. The Head Office of the Bank is located at Juaben, in the Ashanti Region about 30 kilometers away from Kumasi. The Bank is the 93rd to be established in the country and the 18th to be established in the Ashanti Region. The Bank has seven other branches in the Ashanti Region. It has its headquarters at Juaben in Ashanti Region. All the branches have been computerized.

- **Nsutaman Rural Bank Limited** is located at Nsuta in Ahanti region. It has no branch.

- **Mfantseman Community Bank Limited** was registered under the Company's code, 1963. Commenced business on the 8th of August 1996. Its headquarters is at Biriwa in the Central Region. It has seven branches and all have been computerized.

- **Assinman Rural Bank Limited** is located at Assin Manso in Central Region. It has two branches located at Fosu and Ajumako.
- **The Lower Pra Rural Bank Limited** formerly known as the Esemaman Rural Bank Limited was incorporated in Ghana on the 20th day of January 1983. The head office of the bank is at Shama, which is 25km from Takoradi, the Western Regional Capital. The Bank has eleven computerized branches.

- **Western Rural Bank Limited** formerly known as Twin City Rural Bank is set up at the heart of Sekondi in the Western Region of Ghana with license to operate in the rural banking industry. Its headquarters is at Sekondi. It has three other branches.

- **Adansi Rural Bank Limited** is a limited liability company established in 1980 in line with the companies code 1963, Act 179 and operates within the framework and limitations in the manner provided for in the banking Act. The bank has seven branches with the headquarters at Fomena in the Ashanti Region of Ghana. All seven branches are computerized.
- **Amansie West Rural Bank Limited** was established and commissioned for operations on October 22, 1983, at Antoakrom in the Amansie West District of the Ashanti Region. It has one other branch at Ahodwo-Daaban in Ashanti region.

- **Kwamanman Rural Bank Limited** was incorporated in Ghana to carry on the business of banking under the Banking Act, 1970 (Act 339), on the 27th of August, 1982 as the 5th Rural Bank in the Ashanti Region and the 38th in the whole country. It has its headquarters at Kwamang. It has four other branches located in the following areas of Ashanti region: Amakom, Mampong, Nsuta and Old Tafo.
- **Akatakyiman Rural Bank Limited** located at Komenda, Cape Coast in Central Region of Ghana. It has no other branch.
- **Agona Rural Bank Limited** is located in Agona Swedru, in Central Region of Ghana. Its headquarters is located at Agona Kwanyako. It has three other branches located in the following areas – Agona Swedru, Kasoa, Nsaba and Duakwa, all in central Region.

3.8 Computerized Banking Software-Temenos eMerge (T24)

Temenos eMerge (T24) is the computerized accounting software secured by the parent company, ARB Apex Bank Limited for all its affiliated rural banks. Temenos eMerge (T24) is targeted at emerging economies for smaller financial institutions such as small banks, credit unions, mutual societies and a wide array of specialized micro-lenders. It is being referred to as a true non-stop, 24hr, n-tier, scalable, functionally rich, real-time banking application that responds to evolving market needs. T24 supports all major industry standards including J2EE, XML, Web Services, Linux, Unix, Windows, Oracle, DB2. T24 is designed to give financial institutions the flexibility and capacity to deliver on the needs of the community banking environment (Temenos, 2012).

Following the successful automation of all the rural and community banks in Ghana on a single instance of Temenos T24 platform for real time online transaction processing,

through the parent bank, ARB Apex Bank, more banks in Ghana and Nigeria are getting comfort in the use of the banking solution (Okonji, 2014).

DataSoft is an implementation partner of TEMENOS T24 and has worked in a number of successful implementations in the country and abroad.

The ARB in Ghana has increased her T24 concurrent users license to over 2000 to enable her sustain the increased growth experienced as a result of the deployment of the banking solution. This has enabled ARB Apex Bank to deepen her statutory regulation/supervisory competence and also offers better financial solutions to the RCBs through which the teeming population of the rural communities is efficiently serviced. This would also enhance a broader financial intermediation among their rural folks and ensure a wider reach of the rural communities (Okonji, 2014).

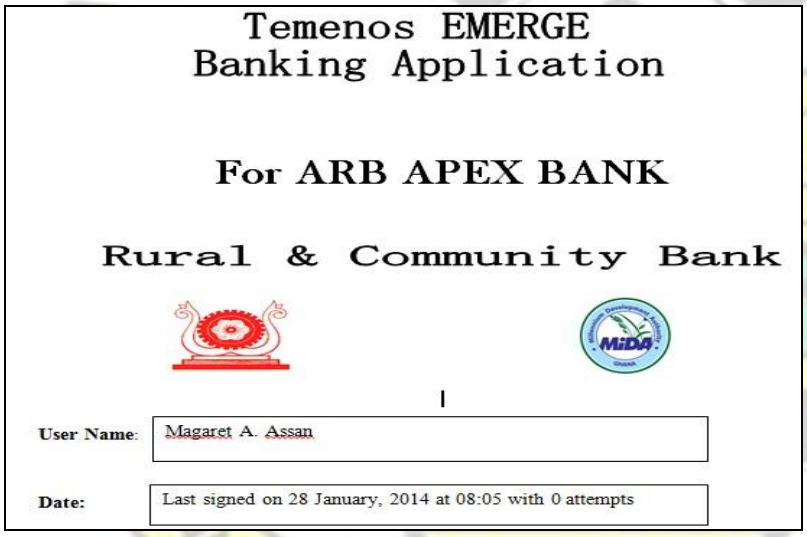


Figure 3.1: A User Screen Interface of T24

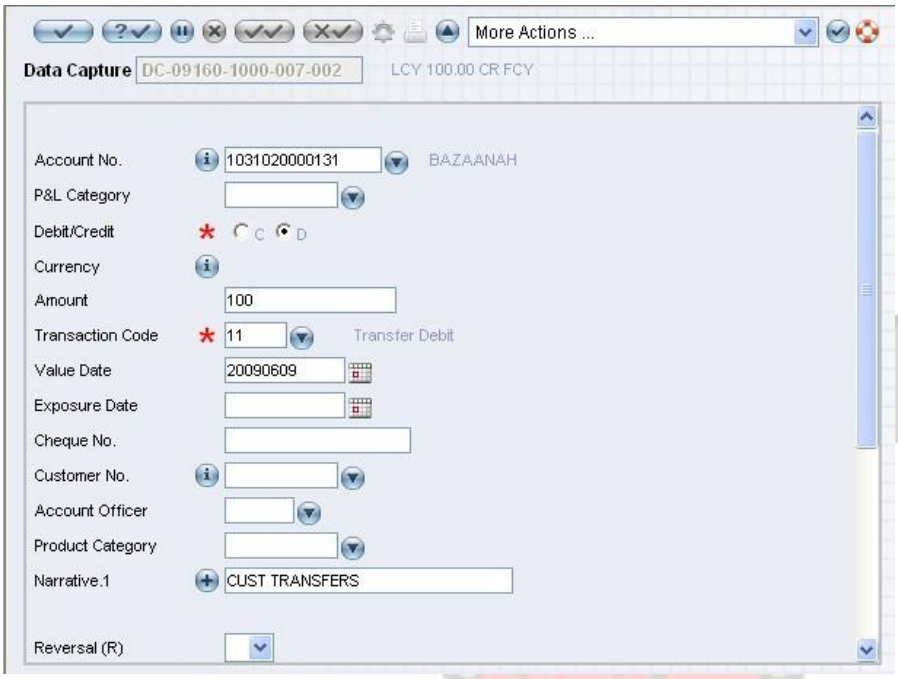


Figure 3.2: A Data Capture Screen for Credit Entry for T24

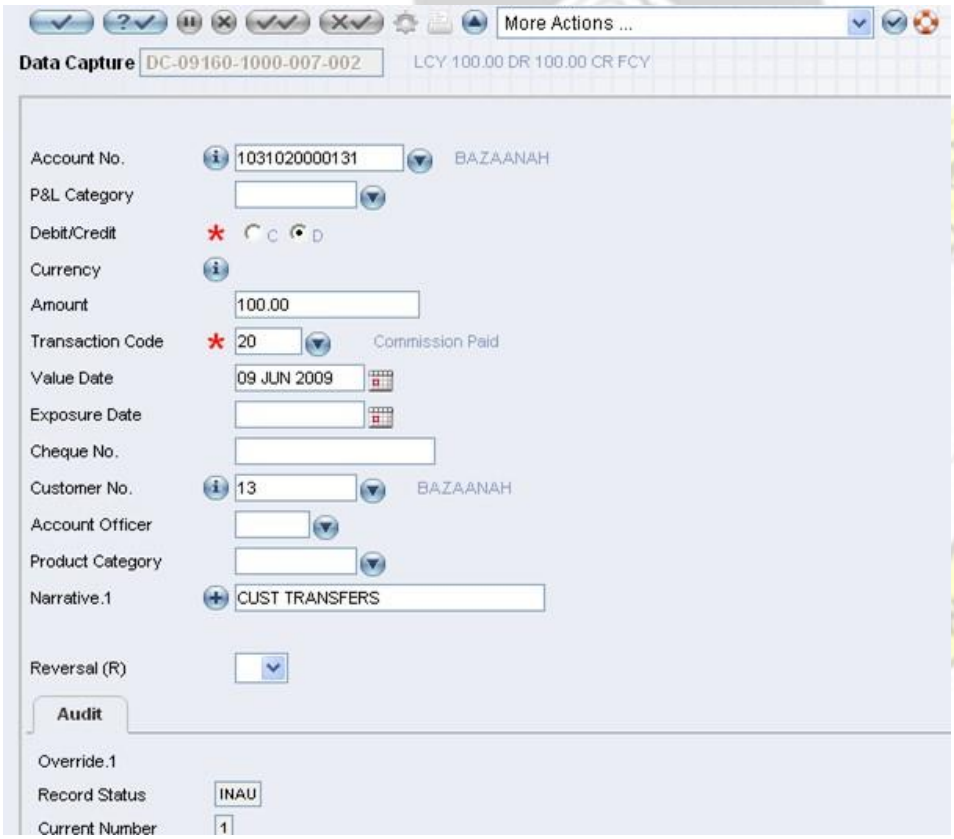


Figure 3.3: A Data Capture Screen for Debit Entry

3.9 Frame Work for IT Audit Access Authorization Controls in Rural Banks

The user access authorizations' policies in the computerized financial institutions comprise the following:

- System Administrator
- Auditor
- Super User
- Authorizer and
- Inputter

KNUST

The System Administrator among other functions, monitors the system for various users to have access to the system on daily basis. The providers of the system (ARB Apex Bank) ensure that the System Administrators only have the access right to set up users and also to view the various activities of the users. The system Administrators also have the sole responsibility of ensuring the following: no external drives are inserted into the computer systems by the users, default passwords are given to the users to change to their own respective passwords on monthly basis, passwords are reset at the middle of every month, access controls' policies are set for all system users, technical reports are sent to ARB Apex Bank where necessary, cold boot the systems and shutdown the systems on daily basis.

The Internal Auditors of the banks have access authorization right to mainly view the various activities of the users of the system. Their major roles entail the following: viewing the list of users of the system on daily basis, viewing list of active users at any given time, viewing users records, checking log of user activities, checking exception reports, checking of Assets and Liability report, checking of Internal Account Balances, checking of Suspense Account and General Ledger Account. The Internal Auditors also have the sole responsibility of ensuring that a manual call-over of all the daily

transactions (cash deposits and cash withdrawals) are done to ascertain that appropriate accounts are debited or credited.

The Super Users are in the persons of Chief Executive Officers, Head of Finance, Branch Managers and Head of Operations. They have the sole access authorization rights to okay all cash transactions into the system on daily basis.

The Authorizers are also in the persons of Supervisors, Accountants and Head of Tellers (Chief Cashiers). They have a limited access authorization rights to okay cash transactions made by the Inputters at the banking yard. They report to the Super Users in all the monetary transactions.

The Inputters are mainly Tellers (Account Officers, Data Clerks) who directly use the system to handle cash deposits and withdrawals' transactions at the banking yard. They also have a limited access authorization rights to okay cash transactions at the counter. They report to the Authorizers.

Figure 3.4 and **Figure 3.5** respectively show screen shots of authorized and unauthorized transactions.


Results 1 - 6 of 6

DATA.CAPTURE - Default Exceptions

Id	Status	Date time	Inputter
DC091601000004001	INAU	20 AUG 09 14:30	22_GEORGE___OFS_TCS
DC091601000004002	INAU	20 AUG 09 14:49	22_GEORGE___OFS_TCS
DC091601000007001	INAU	20 AUG 09 15:01	22_GEORGE___OFS_TCS
DC091601000007002	INAU	20 AUG 09 15:04	22_GEORGE___OFS_TCS
DC091601000008001	INAU	21 AUG 09 15:02	22_INPUTTER___OFS_TCS
DC091601000008002	INAU	21 AUG 09 15:19	22_GEORGE___OFS_TCS

Figure 3.4: Authorised Transaction Entry Screen

Results 1 - 4 of 4

UNAUTHORISED DATA CAPTURE ENTRY LIST

Batch : DC09160

TC Account Number Short Title Value Date CCY Amount in CCY Narrative

TRANS.CODE	ACCT.OR.CAT		ACCT.OR.CAT.TIT	VAL.DATE	LOC.CCY	LCY.CCY.AMT	PSIGN	NARR
70	52005		Cheque Charges	09 JUN 2009	GHS	10.00	C	
	20 AUG 2009	14:30						
20	1031020000211		AYAMABA	09 JUN 2009	GHS	10.00	D	CHARGES FOR CHQ ISSUED.
	20 AUG 2009	14:49						
61	1031020000211		AYAMABA	09 JUN 2009	GHS	100.00	C	CUST TRANSFERS
	20 AUG 2009	15:01						
20	1031020000131		BAZAANAH	09 JUN 2009	GHS	100.00	D	CUST TRANSFERS
	20 AUG 2009	15:04						
	BATCH TOTAL	LCY	110.00 DR	110.00 CR				
		FCY	0.00 DR	0.00 CR				
	ENTRY TOTAL	4						

Figure 3.5: Unauthorized Transaction Entry Screen

3.2.2 Hierarchy of Category of System Users in Computerized Rural Banks

The model below shows the hierarchy of system users in relation to IT Access Controls' authorization rights that restrict access to banks information and systems in accordance with the organizations' information security and privacy policies and standards.

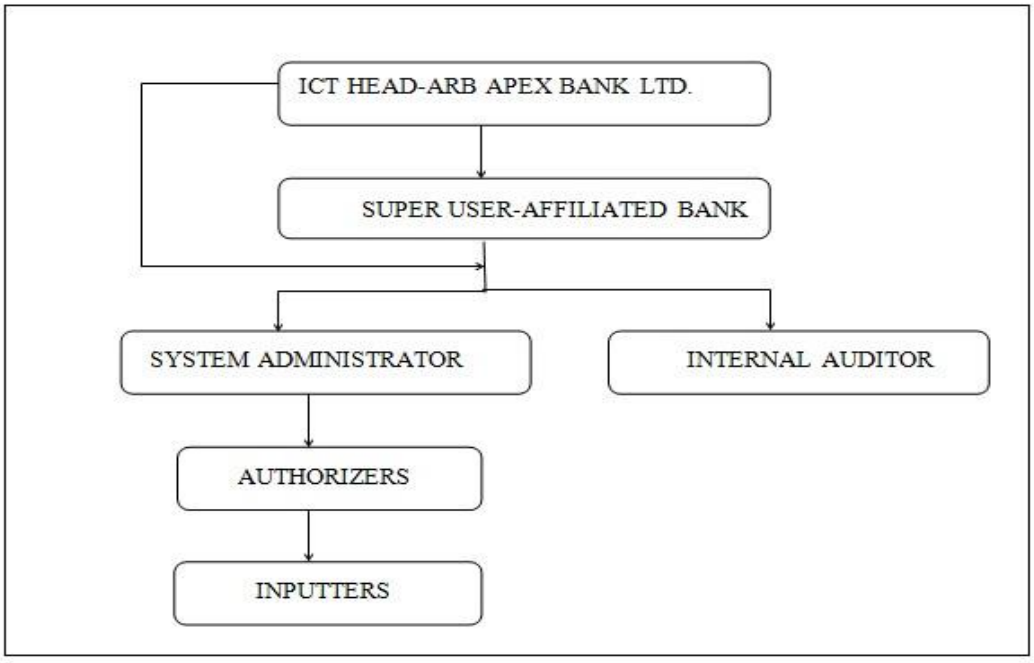
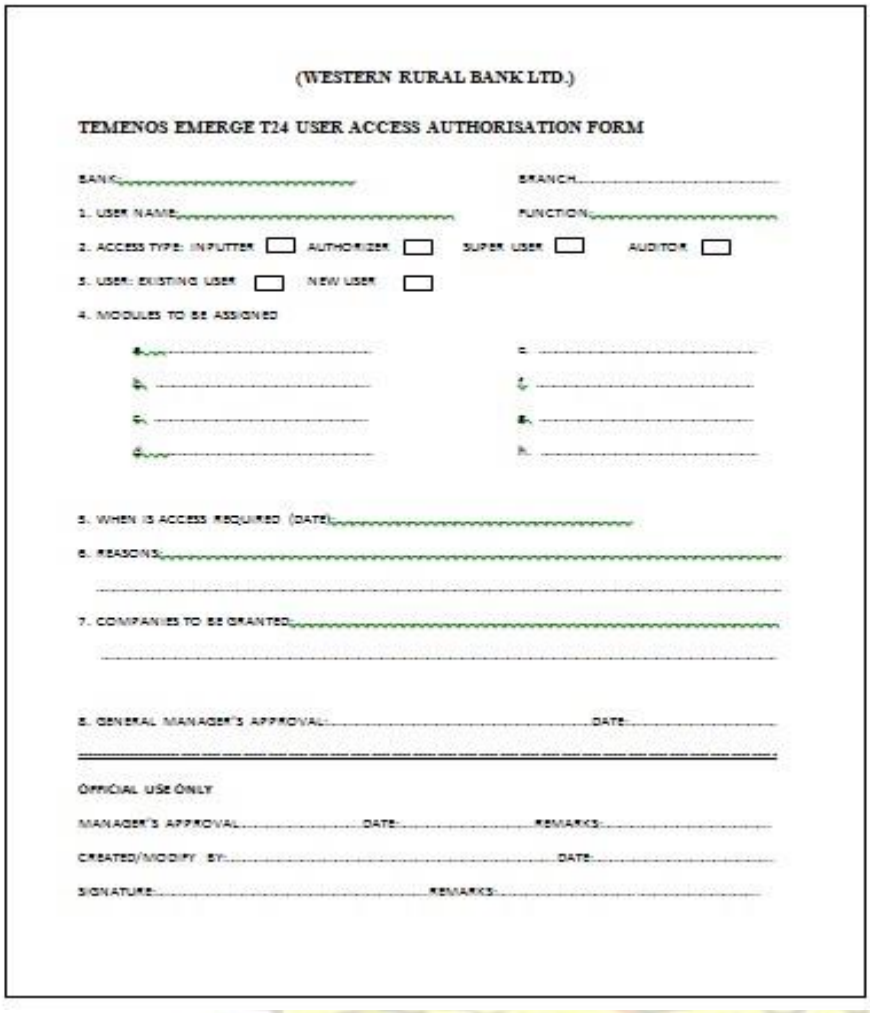


Figure 3.6: Hierarchy of Category of System Users



(WESTERN RURAL BANK LTD.)

TEMENOS EMERGE T24 USER ACCESS AUTHORISATION FORM

BANK:..... BRANCH:.....

1. USER NAME:..... FUNCTION:.....

2. ACCESS TYPE: INPUTTER ☐ AUTHORIZER ☐ SUPER USER ☐ AUDITOR ☐

3. USER: EXISTING USER ☐ NEW USER ☐

4. MODULES TO BE ASSIGNED

a. ..... e. .....

b. ..... f. .....

c. ..... g. .....

d. ..... h. .....

5. WHEN IS ACCESS REQUIRED (DATE):.....

6. REASONS:.....

.....

7. COMPANIES TO BE GRANTED:.....

.....

8. GENERAL MANAGER'S APPROVAL:..... DATE:.....

OFFICIAL USE ONLY

MANAGER'S APPROVAL..... DATE:..... REMARKS:.....

CREATED/MODIFY BY:..... DATE:.....

SIGNATURE:..... REMARKS:.....

Figure 3.7: User Access Authorization Form. (A Source Document from Western Rural Bank Ltd.)

CHAPTER FOUR

PRESENTATION OF FIELD DATA

4.1 Introduction

This chapter of the research presents collected primary and secondary data from the sampled sixteen rural banks selected from three regions (Ashanti, Western and central)

in Ghana. The sampled financial institutions selected from Ashanti Region are Adansi Rural Bank-Fomena, Amansie West Rural Bank Ltd-Antoakrom, Askore Rural Bank-Asokore, Atwima Kwanwoma Rural Bank Ltd-Atwima, Bosomtwe Rural Bank Ltd.Kuntanase, Juaben Rural Bank Ltd.-Juaben, Kumawuman Rural Bank Ltd-Bomso, Kwamanman Rural Bank Ltd-Kwaman, Atwima Rural Bank Ltd.-Foase. Nsutaman Rural Bank Ltd-Nsuta. The selected banks from the Central region are Agona Rural Bank Ltd.-Agona Kwannyako, Assinman Rural Bank Ltd-Assin Manso, Mfanseman Commercial Bank Ltd-Biriwa, Those financial institutions selected from the Western Region are Ahantaman Rural Bank Ltd. -Agona Nkwanta, and Western Rural Bank Ltd-Sekondi .

4.2 Demography

The study observed that the demography features of respondents were relevant in looking at gender of respondents, position held by respondents in the financial institution, age, educational status and field of study of sampled respondents.

4.2.1 Gender of Respondents

The study sampled one hundred and twenty respondents working in financial institutions (rural banks in Ghana) of which 67 percent were Males and 33 percent Females. Respondents from the field data collected were holding positions such as Branch managers, Clerks, Tellers, Customer service person, Auditors, finance officer, IT Officers among other positions in the various financial institutions.

4.2.2 Educational Status of Respondents

Education is the driving force of every institution, with this it was worth knowing the educational status of the sampled respondents of the study. From the 120 sampled respondents, 90 percent were tertiary education products, 6 percent second cycle

education graduates and 4 percent are products from other disciplines including professionals from the professional certified institutions. Banking being opportunity grounds for individuals with business background, 66 percent of the sampled respondents were from business background and 6 percent business and computer based background. For the research it was worth interviewing respondents with Accounting Information System background.

KNUST

4.3 Information Technology Audit Control Systems

As explained in the literature review, IT Audit is meant to evaluate the IT control systems that are put in place to safeguard organizational transactions and overall business setups. In this regard IT audit controls are objectively used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties.

4.3.1 Information Technology Audit Controls Used in Financial Institutions

IT Audit controls as reviewed in the literature comprised series of components, including preventive, detective and corrective audit controls. In carrying out the study, IT Audit controls assessed in the various banks included Access Controls, Monitoring Controls, Asset Identification Controls, Asset and Identification Management Controls, Backup and Recovery Controls, Disaster Recovery Controls, Program Change Controls, Network Controls, Computer Operations Controls, Internet and E-Commerce Controls, Telecommunication Controls and Database Controls.

From the field data it was crystal clear that all the sampled computerized financial institutions used the assessed IT Audit controls in their institutions. On the average 9.2 percent (SD 0.7) of the sixteen sampled financial institutions had control systems. In this, 97.5 percent of the sampled respondents responded “YES” to using the above control

systems in their financial institutions and 2.5 percent responded “NO”. The above breakdown shows high adherence and relevance associated with IT Audit controls in financial institutions.

However, Internet and E-commerce controls assessed were the least controls used. This shows that there is high usage of the other IT Audit controls by the banks (which represent about 97.5 percent among the controls used) as opposed to internet and Ecommerce controls (2.5 percent). Thus, IT Audit controls regarding internet and ecommerce need to be seriously looked into for their full integration into the banks daily financial transactions.

The table below shows the responses of respondents on usage of IT Audit controls by the sampled financial institutions.

Table 4.3.1 Other IT Audit Controls Used by Financial Institutions

Control Systems	**Frequency of Responses**					
	Yes	**(%)**	**No**	**(%)**	**Don’t Know (%)**	
Access Controls	119	99.2	1	0.8	0	0
Monitoring Controls	118	98.3	2	1.7	0	0
Asset Identification Controls	116	96.7	4	3.3	0	0
Asset and Identity Management Control	118	98.3	2	1.7	0	0
Backup and Recovery control	118	98.3	2	1.7	0	0
Disaster Recovery Controls	116	96.7	4	3.3	0	0
Program Change Control	115	95.8	5	4.2	0	0
Network Control	115	95.8	5	4.2	0	0

Computer Operations Controls	116	96.7	3	2.5	1	0.8
Internet and E-commerce	3	2.5	116	96.7	1	0.8
Telecommunication Controls	4	3.3	115	95.8	1	0.8
Database Controls	115	95.8	4	3.3	1	0.8

Source: Field Work 2014.

KNUST

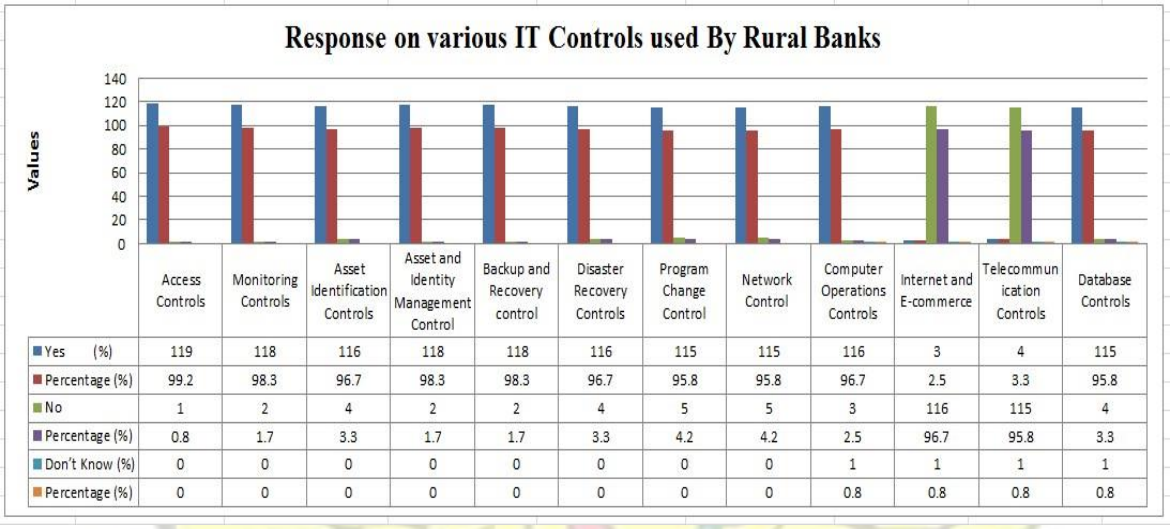


Figure 4.3.1: Other IT Audit Controls Used by the Rural Banks in Ghana

4.3.2 Extent of Agreement on the usage of Access Controls

Access controls comprised Authorization controls and Authentication controls. As explained in the Literature review. Authorization controls basically provide the functionality to verifying that a certain combination of ID and password has been granted permission to access a system. Authentications controls verify that the login (ID/password) belongs to the person who is attempting to gain access, i.e., users are who they say they are. In the study the respondents were asked to indicate the extent to which they agree in the usage of systems' access controls in their respective institutions. Statistically, the collected field data revealed the following. About 73.1 percent of respondents strongly agreed on the usage of access controls. In addition a considerable

number (21.8 percent of respondents) also agreed on the usage of IT Audit access controls. About 3.2 percent of respondents disagreed on the IT Audit access controls usage. A very low percentage of respondents (1.2 percent) strongly disagreed on the usage of IT Audit access controls. Insignificantly 0.7 percent of respondents seemed oblivious of existence of such IT Audit access controls in the organizations.

The various levels of responses of the respondents on the usage of IT Audit access controls were the true reflection of the systems' audit trail daily reports. Needless to say, respondents' high agreement on the usage of IT Audit access controls were indicative of the fact that the access controls contribute significantly to the effective functioning of institutions daily activities or transactions.

Furthermore, investigation on other IT Audit systems' controls used in the questionnaires also affirmed that the banks really employ these IT Audit controls on daily basis to ensure that their business objectives and goals are met as depicted by the respective respondents' responses.

Figures and Tables below show the extent of agreement on the usage of IT Audit Access controls from respondents in their respective organizations

Table 4.3.2: Extent of Agreement on the usage of IT Audit Access Controls

Level of Agreement	Frequency	Percentage
Agree	26.2	21.8
Strongly Agree	87.7	73.1
Disagree	3.8	3.2
Strongly Disagree	1.4	1.2
Not Sure	0.8	0.7
Total	120.0	100.0

Source: Field Survey, 2014.

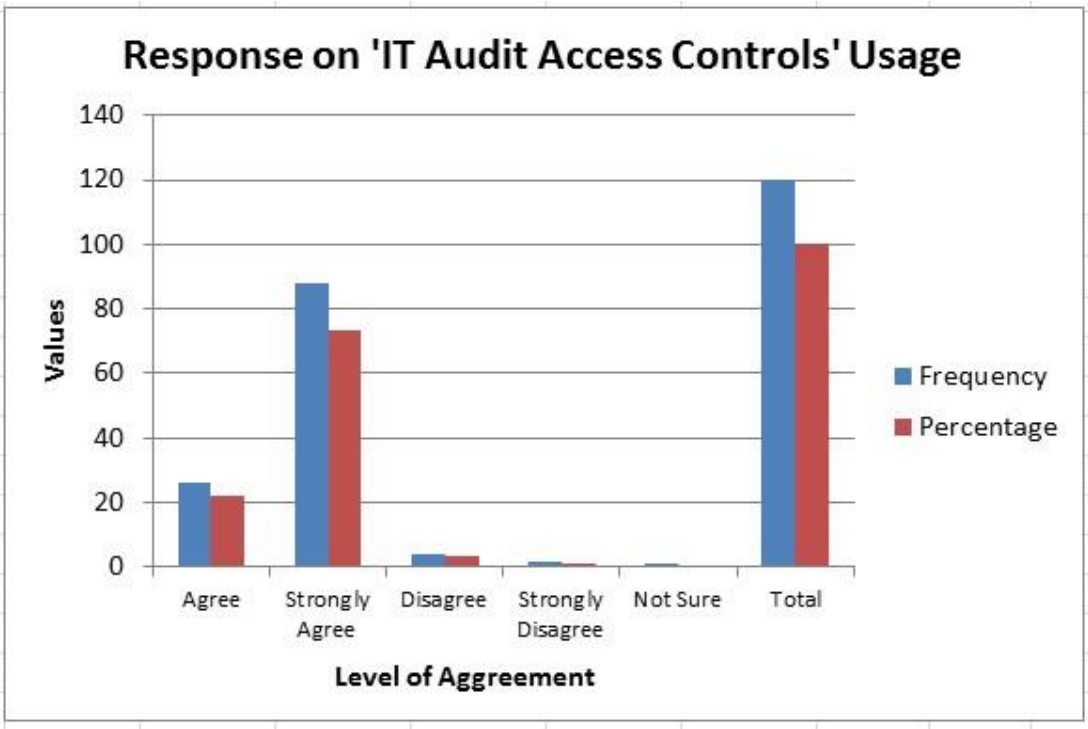


Figure 4.3.2 Extent of Agreement on the usage of Access Controls

4.3.3 T24 Banking Software Access Controls

In carrying out the research study it was worth considering the banking software used by the banks and IT audit controls associated with the T24 banking software. The collected field data revealed that all the sampled rural banks used 'T24' computerized Accounting Software.

In assessing the IT audit access controls associated with the T24 banking software, the study discovered that about 93.3 percent of the respondents used passwords in protecting their personal computers. About 6.7 percent of respondents irresponsibly did not protect their PCs with passwords. Additionally, those who use passwords in protecting their PCs, 78.0 percent readily agreed that all assigned passwords did have expiry date. However, 22.0 percent of the respondents admittedly responded 'NO' to assigned passwords having expiry date.

Significantly, about 95.0 percent of respondents in the sampled financial institutions also revealed that they hardly experience unauthorized electronic access to their working PCs.

The 5.0 percent of the respondents who experienced some electronic access to their working PCs without their prior permissions were as a result of mere human negligence. This made them very alarmed since they were not oblivious of the possible consequences that these acts of negligence would lead to. Thus, this accounted for the few unauthorized accesses recorded in system log reports (audit trails) in the sampled financial institutions.

Table 4.3.3: T24 Banking Software Access Controls (Regarding Password Usage)

Access Controls	Frequency of Responses					
	Yes	(%)	No	(%)	Don't Know (%)	
Password Usage	112	93.3	8	6.7	0	0
Password Expiry Date	93.6	78.0	36.4	22.0	0	0
Unauthorized Access	6	5.0	114	95.0	0	0

Source: Field Work 2014.

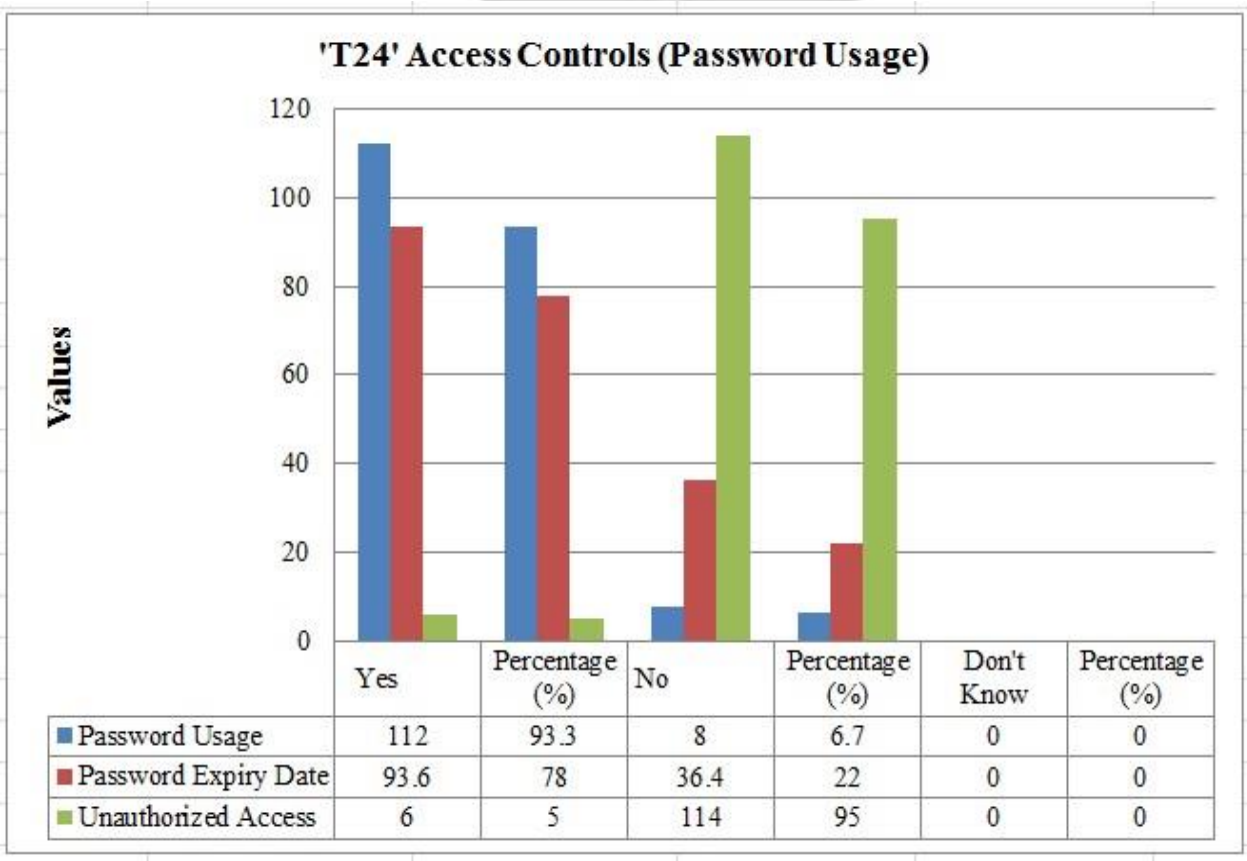


Figure 4.3.3: T24 Banking Software Access Controls (Regarding Password Usage)

4.3.4 Other Tables and their Respective Figures

The following are the other Tables and Figures derived from the research study.

Table 4.3.4: Agreement Level on Usage of 'Unique Password'

Level of Agreement	Frequency	Percentage
Agree	21	17.5
Strongly Agree	96	80.0
Disagree	1	0.8
Strongly Disagree	0	0.0
Not Sure	2	1.7
Total	120	100.0

Source: Field Survey, 2014.

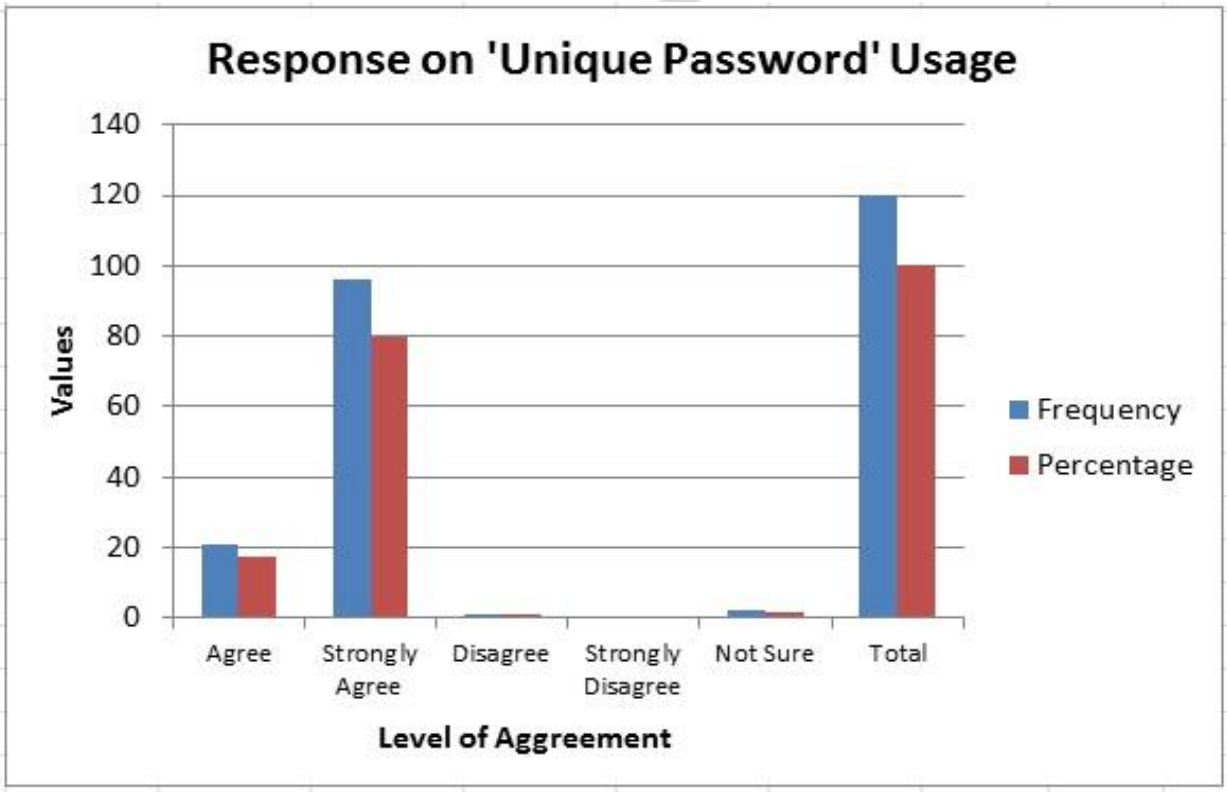


Figure 4.3.4 Extent of Agreement on 'Unique Password' Usage

Table 4.3.5: The IT Audit Access controls on 'periodic passwords change'

Level of Agreement	Frequency	Percentage
Agree	19	15.8
Strongly Agree	98	81.7
Disagree	2	1.7
Strongly Disagree	1	0.8
Not Sure	0	0.0
Total	120	100.0

Source: Field Survey, 2014.

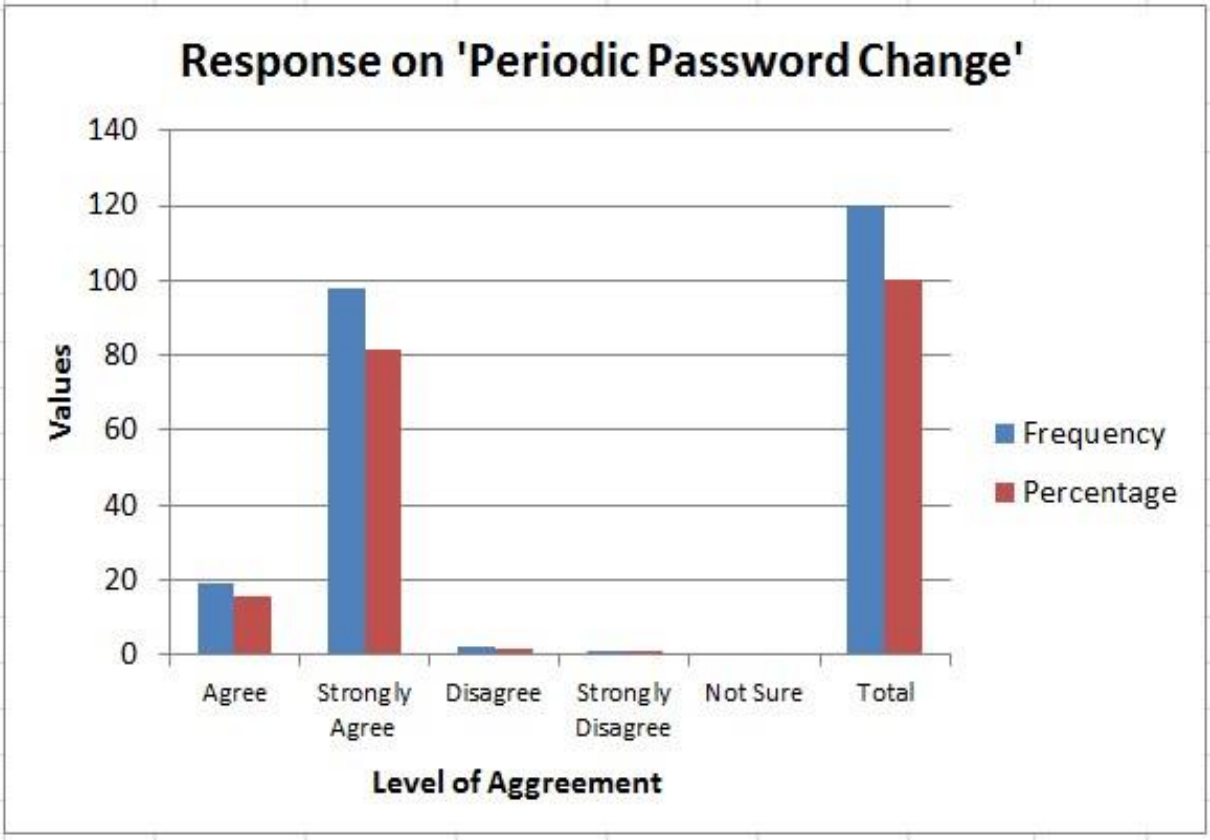


Figure 4.3.5: IT Audit Access controls on 'Periodic Passwords Change'

Table 4.

3.6: The IT Audit Access controls on 'cancellation or access rights modification upon an employee's termination or transfer in a timely manner'

Level of Agreement	Frequency	Percentage
Agree	14	11.7
Strongly Agree	101	84.1
Disagree	3	2.5
Strongly Disagree	0	0.0
Not Sure	2	1.7
Total	120	100.0

Source: Field Survey, 2014.

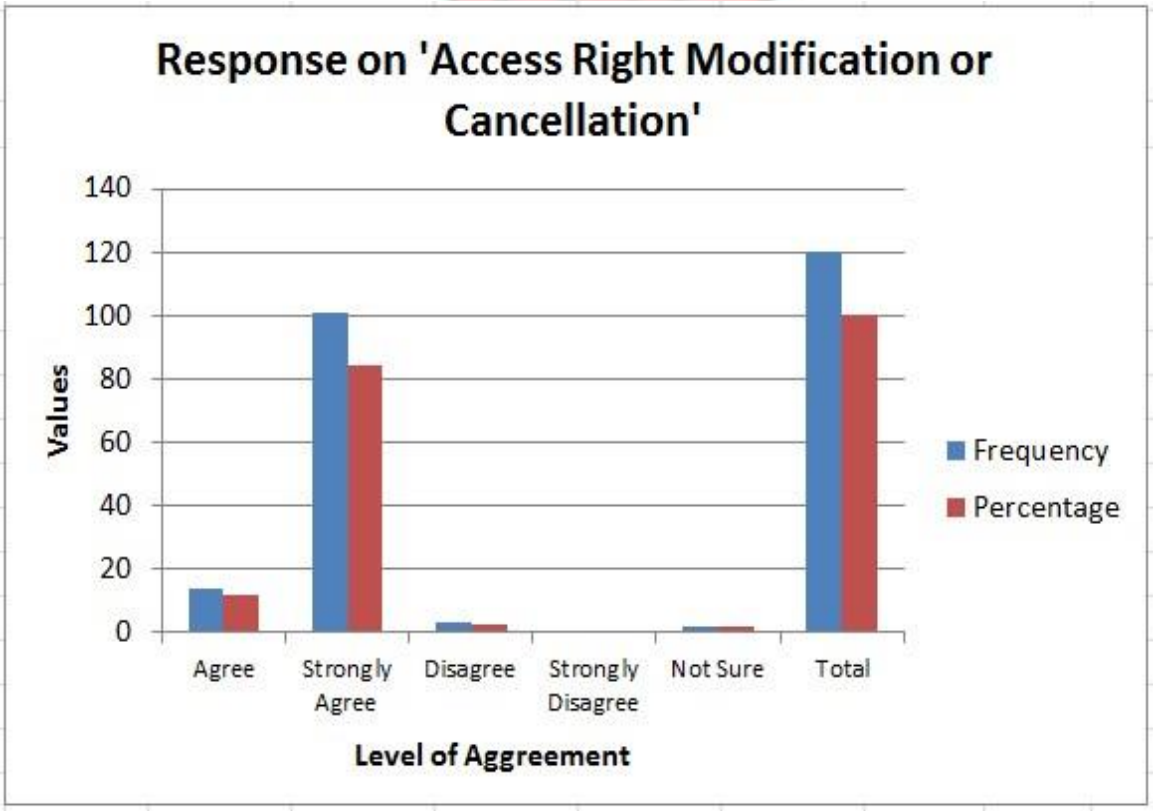


Figure 4.3.6 : IT Audit Access Controls on 'Access Right Modification or

Cancellation on Employee's Termination orTransfer'

Table 4.3.7: IT Audit Controls on 'Review of System Generated Reports by the System Administrator'

Level of Agreement	Frequency	Percentage
Agree	22	18.3
Strongly Agree	92	76.7
Disagree	2	1.7
Strongly Disagree	1	0.8
Not Sure	3	2.5
Total	120	100.0

Source: Field Survey, 2014.

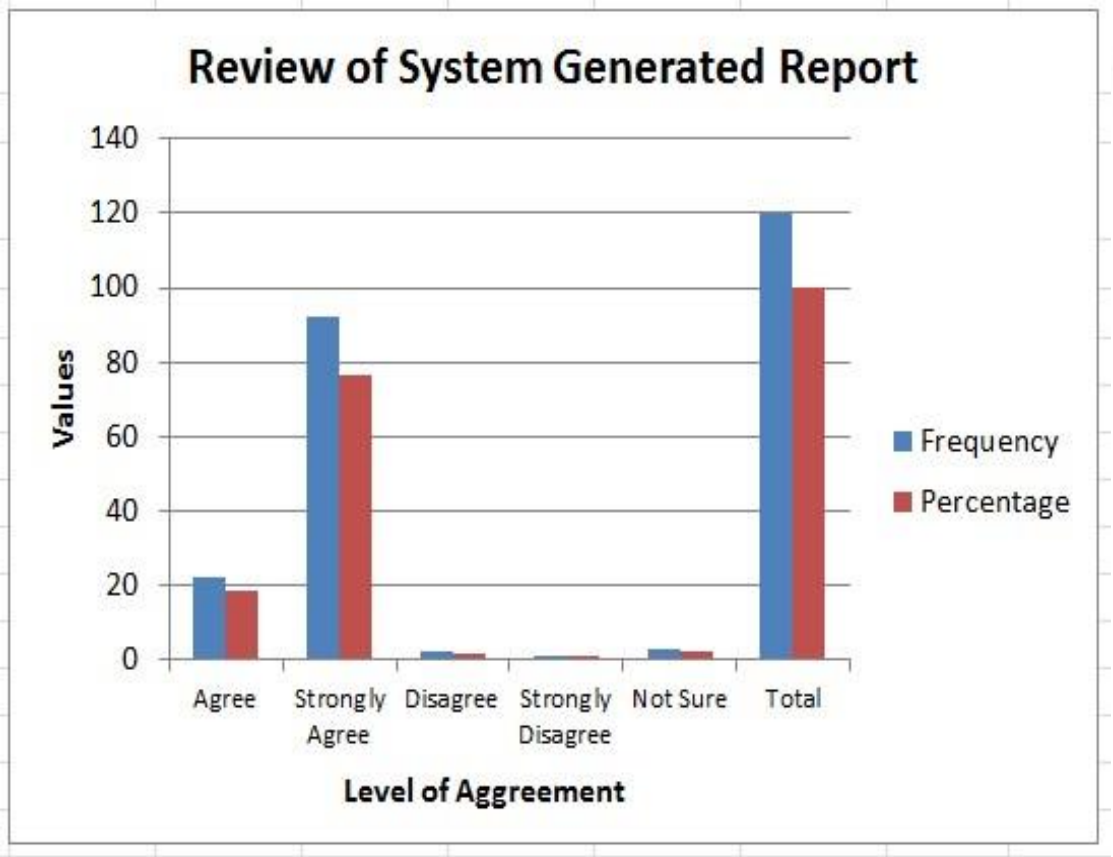


Table 4.

Figure 4.3.7: IT Audit Controls on 'Review of System Generated Reports

8: IT Audit Controls on 'The system generated reports able to show authorized and unauthorized accesses to the banking software'

Level of Agreement	Frequency	Percentage
Agree	27	22.5
Strongly Agree	89	74.2
Disagree	1	0.8
Strongly Disagree	2	1.7
Not Sure	1	0.8
Total	120	100.0

Source: Field Survey, 2014.

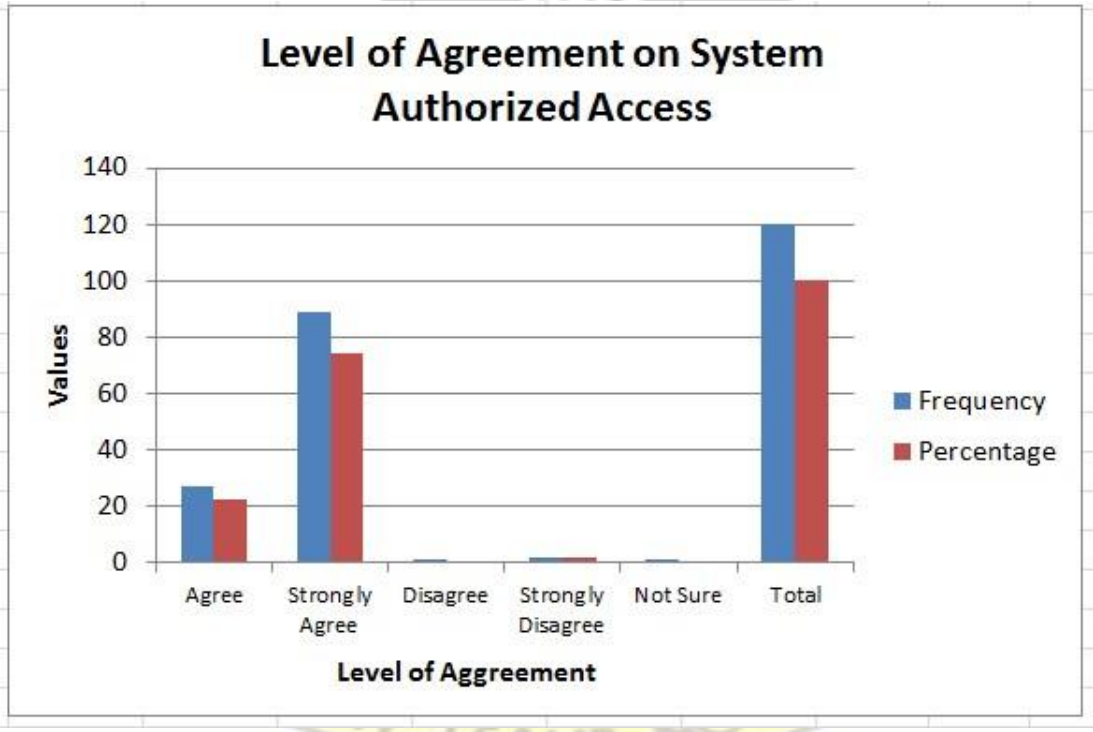


Figure 4.3.8: IT Access Controls on 'Level of Agreement on Authorized and Unauthorized accesses to the banking software'

Table 4.

3.9: IT Audit Controls on 'Procedures in place to follow up on these systems generated reports'

Level of Agreement	Frequency	Percentage
Agree	24	20.0
Strongly Agree	90	75.0
Disagree	1	0.8
Strongly Disagree	3	2.5
Not Sure	2	1.7
Total	120	100.0

Source: Field Survey, 2014.

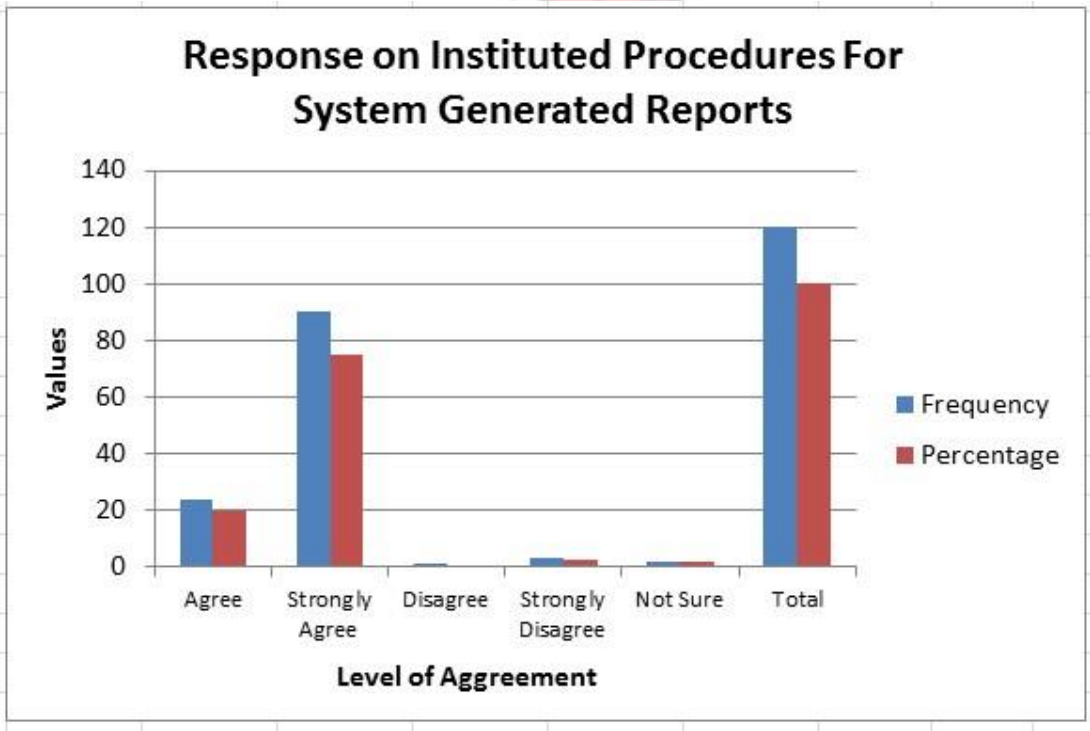


Figure 4.3.9: IT Audit Controls on 'Procedures for System Generated Reports'

3.10: IT Audit controls on 'Systems put in place to safeguard the institution's operations against perceived threats or impending dangers'

Level of Agreement	Frequency	Percentage
Agree	23	19.2
Strongly Agree	93	77.4
Disagree	2	1.7
Strongly Disagree	0	0.0
Not Sure	2	1.7

Table 4.

Total	120	100.0

Source: Field Survey, 2014.

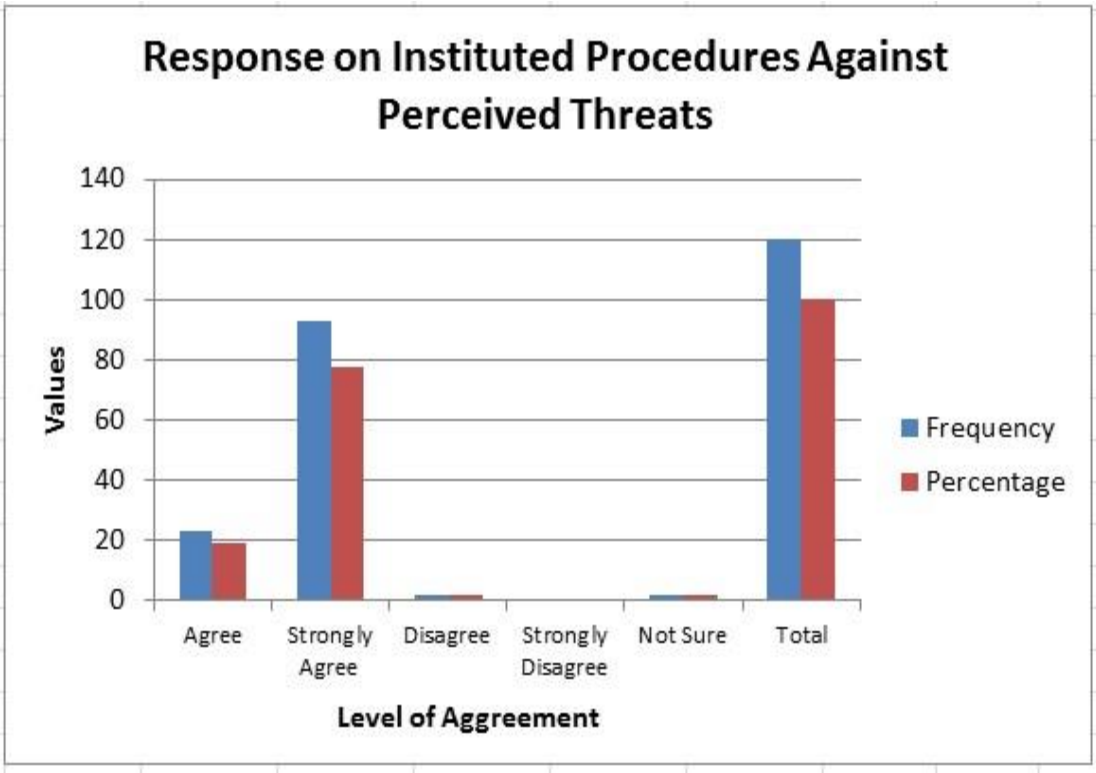


Figure 4.3.10: IT Audit controls against 'Perceived Threats'

3.11: IT Audit controls on 'Shareholders of the bank having absolute confidence in IT audit controls'

Level of Agreement	Frequency	Percentage
Agree	26	21.7
Strongly Agree	90	75.3
Disagree	1	0.5
Strongly Disagree	1	0.8
Not Sure	2	1.7
Total	120	100.0

Source: Field Survey, 2014.

Table 4.

Figure 4.3.11: 'Shareholders Confidence' in IT Audit Controls

3.12: IT Audit controls on 'System users having absolute confidence in the security offered by the IT audit controls'

Level of Agreement	Frequency	Percentage
Agree	22	18.4
Strongly Agree	93	77.5
Disagree	1	0.8
Strongly Disagree	1	0.8
Not Sure	3	2.5
Total	120	100.0

Source: Field Survey, 2014.

Table 4.

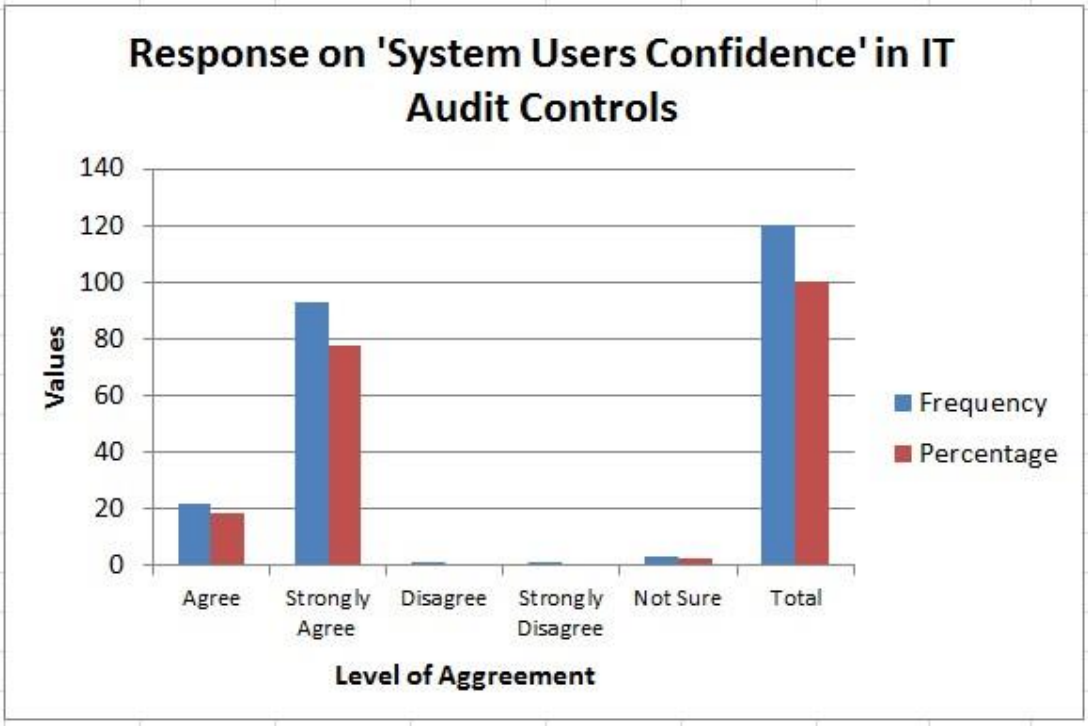


Figure 4.3.12: 'System Users Confidence' in IT Audit Controls

3.13 IT Audit controls on 'Banking customers having absolute confidence in the computerized system being used to serve them'

Level of Agreement	Frequency	Percentage
Agree	26	21.7
Strongly Agree	88	73.4
Disagree	1	0.8
Strongly Disagree	1	0.8
Not Sure	4	3.3
Total	120	100.0

Source: Field Survey, 2014.

Table 4.

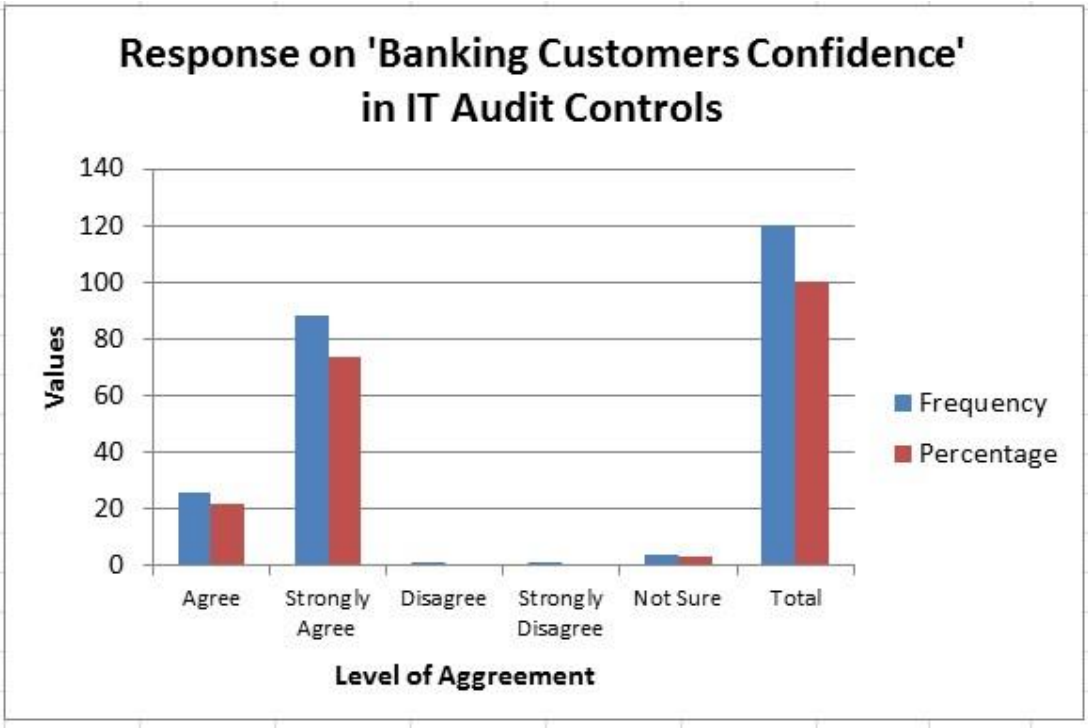


Figure 4.3.13: 'Banking Customers Confidence' in IT Audit Controls

3.14: IT Audit controls on 'Users sharing the view that computerized banking software has contributed greatly to reducing banking crimes or frauds'

Level of Agreement	Frequency	Percentage
Agree	27	22.5
Strongly Agree	87	72.5
Disagree	3	2.5
Strongly Disagree	1	0.8
Not Sure	2	1.7
Total	120	100.0

Source: Field Survey, 2014.

Table 4.

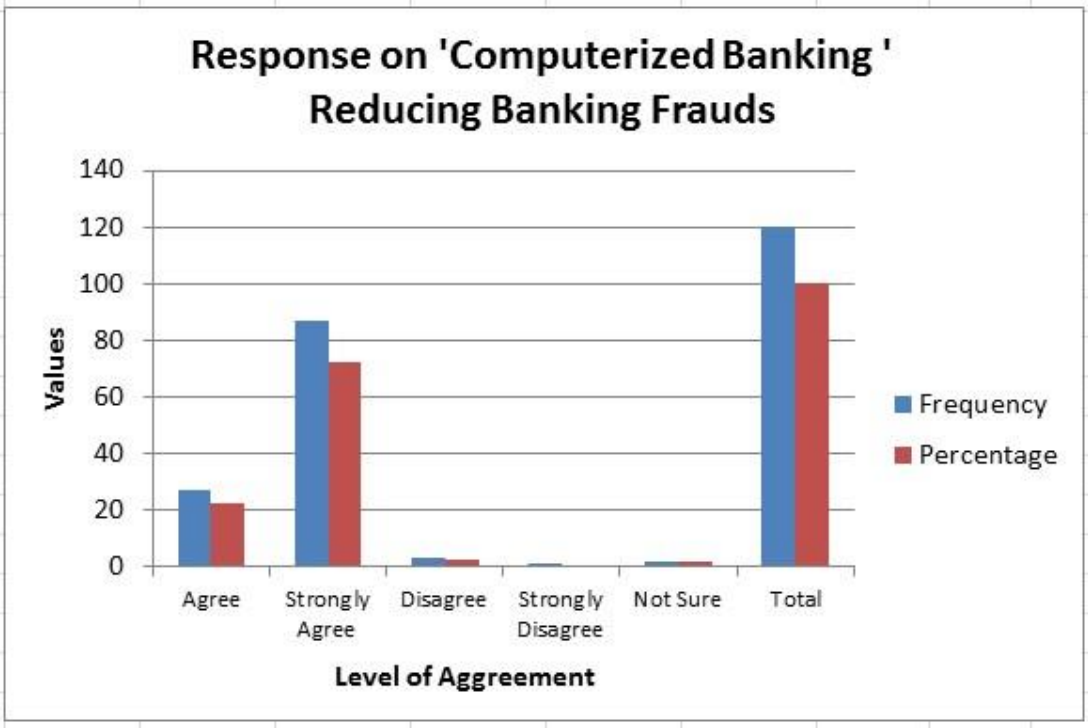


Figure 4.3.14: 'Computerized Banking' Reducing Banking Frauds

3.15: IT Audit controls on 'There are still security challenges in spite of the IT audit security control systems being used'

Level of Agreement	Frequency	Percentage
Agree	18	15.0
Strongly Agree	72	60.0
Disagree	21	17.5
Strongly Disagree	1	0.8
Not Sure	8	6.7
Total	120	100.0

Source: Field Survey, 2014.

Table 4.

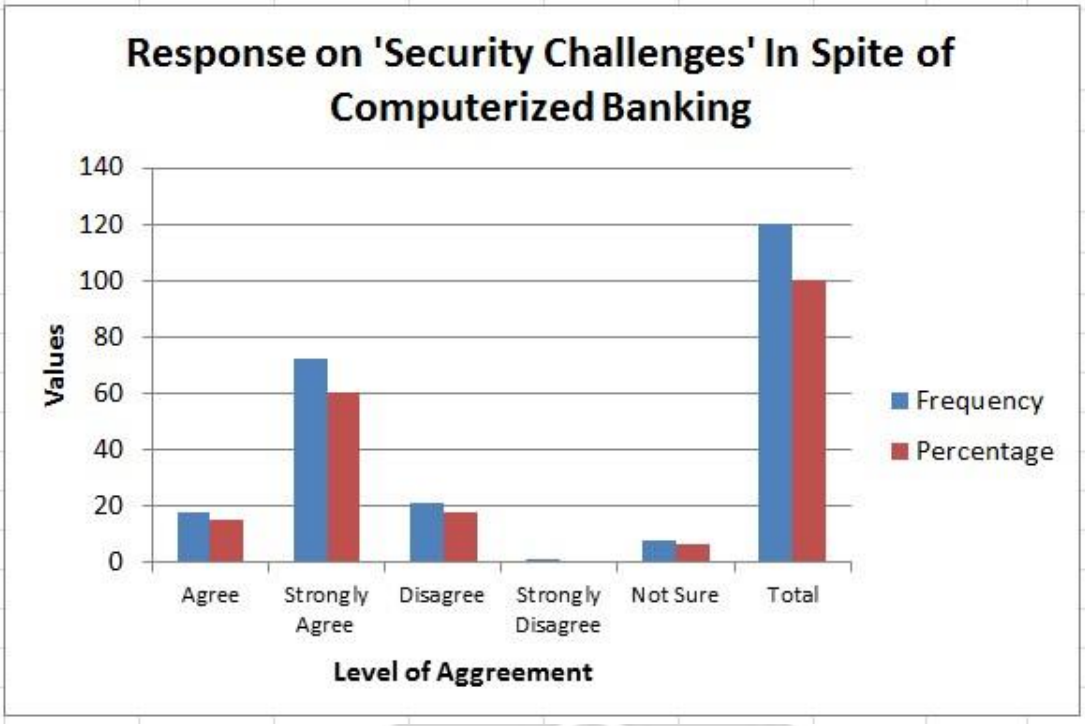


Figure 4.3.15: 'Computerized Banking' Reducing Banking Frauds

4.4.1 Security Challenges

The research conducted on the sampled financial institutions also depicted that the institutions have some security challenges in spite of IT audit security controls being used. In the study, security challenges such as Bank Impersonation, Cheque Kiting, Forgery and Altered cheques, Accounting Fraud, Identity Theft, Fraudulent Loans, Forged Documents, Fictitious Bank Inspector, Cheque Fraud and Phishing were

assessed. This was done to find out whether or not the presence of IT audit security controls employed by the financial institutions were effective in addressing these security challenges such as above.

Statistically the respondents' responses (50.4 percent) strongly agreed to dangers posed by these security challenges in their respective financial institutions as illustrated by Figure 4.4.1 and Table 4.4.1 below. Thus, the above underscores the need to strengthen IT Audit security controls in financial institutions.

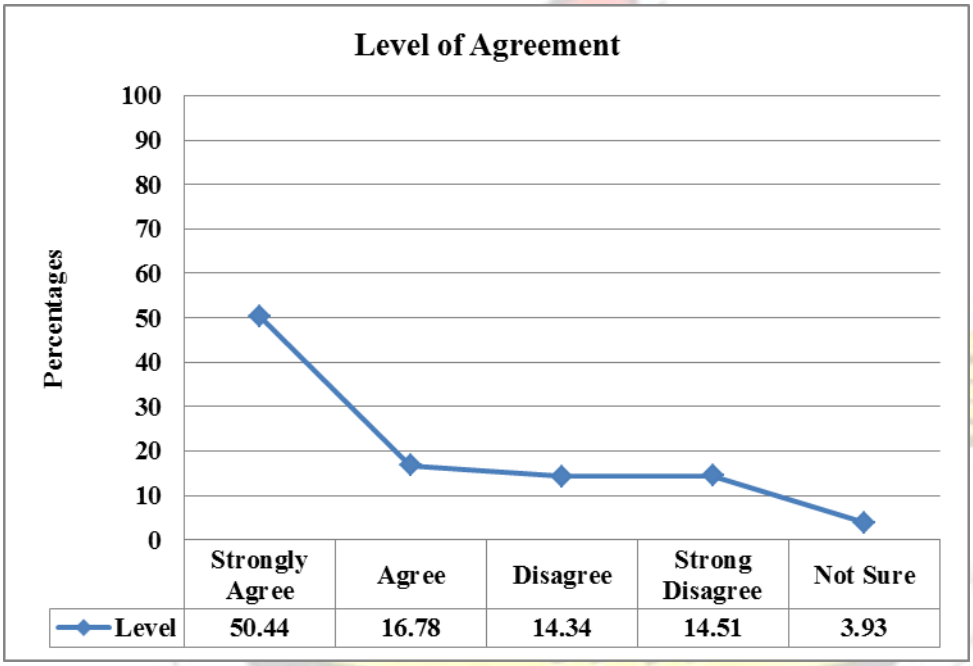


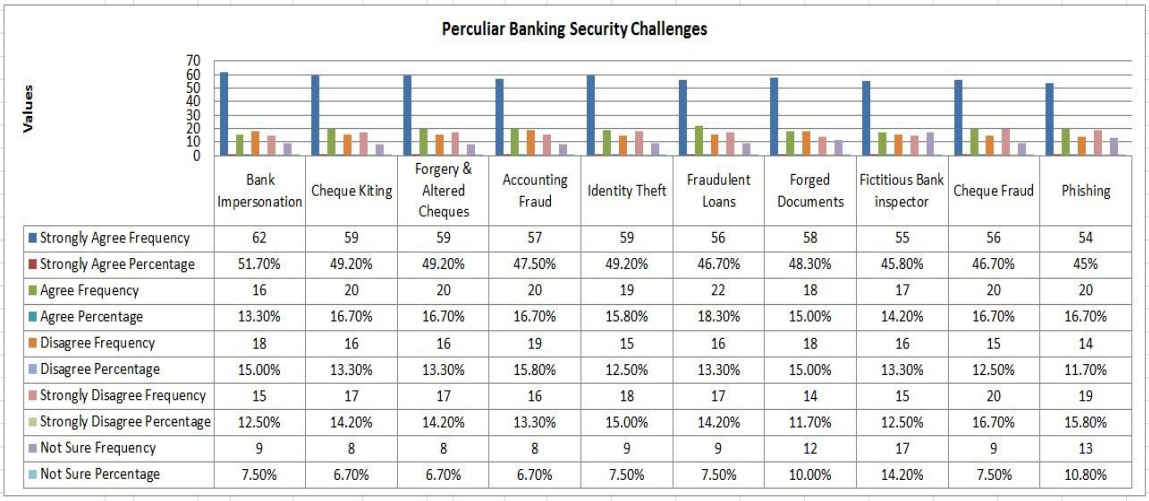
Figure 4.4.1: Extent of Respondents' Responses on Security Challenges.

Table 4.4.1: Unit of Inquiry for Security Challenges

Security Challenges	Strongly Agree		Agree		Disagree		Strongly Disagree		Not Sure	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Bank Impersonation	62	51.7%	16	13.3%	18	15.0%	15	12.5%	9	7.5%
Cheque Kiting	59	49.2%	20	16.7%	16	13.3%	17	14.2%	8	6.7%
Forgery & Altered Cheques	59	49.2%	20	16.7%	16	13.3%	17	14.2%	8	6.7%
Accounting Fraud	57	47.5%	20	16.7%	19	15.8%	16	13.3%	8	6.7%
Identity Theft	59	49.2%	19	15.8%	15	12.5%	18	15.0%	9	7.5%
Fraudulent Loans	56	46.7%	22	18.3%	16	13.3%	17	14.2%	9	7.5%
Forged Documents	58	48.3%	18	15.0%	18	15.0%	14	11.7%	12	10.0%
Fictitious Bank inspector	55	45.8%	17	14.2%	16	13.3%	15	12.5%	17	14.2%
Cheque Fraud	56	46.7%	20	16.7%	15	12.5%	20	16.7%	9	7.5%
Phishing	54	45%	20	16.7%	14	11.7%	19	15.8%	13	10.8%

Source: Field Survey, 2014.

KNUST
WJSANE NO BADWENMA



	Bank Impersonation	Cheque Kiting	Forgery & Altered Cheques	Accounting Fraud	Identity Theft	Fraudulent Loans	Forged Documents	Fictitious Bank inspector	Cheque Fraud	Phishing
Strongly Agree Frequency	62	59	59	57	59	56	58	55	56	54
Strongly Agree Percentage	51.70%	49.20%	49.20%	47.50%	49.20%	46.70%	48.30%	45.80%	46.70%	45%
Agree Frequency	16	20	20	20	19	22	18	17	20	20
Agree Percentage	13.30%	16.70%	16.70%	16.70%	15.80%	18.30%	15.00%	14.20%	16.70%	16.70%
Disagree Frequency	18	16	16	19	15	16	18	16	15	14
Disagree Percentage	15.00%	13.30%	13.30%	15.80%	12.50%	13.30%	15.00%	13.30%	12.50%	11.70%
Strongly Disagree Frequency	15	17	17	16	18	17	14	15	20	19
Strongly Disagree Percentage	12.50%	14.20%	14.20%	13.30%	15.00%	14.20%	11.70%	12.50%	16.70%	15.80%
Not Sure Frequency	9	8	8	8	9	9	12	17	9	13
Not Sure Percentage	7.50%	6.70%	6.70%	6.70%	7.50%	7.50%	10.00%	14.20%	7.50%	10.80%

Figure 4.4.2: Extent of Respondents' Responses on Security Challenges

4.4.2 Breaches in IT Audit Controls

As outlined in the Literature review, a breach in IT audit security controls is an act from outside an IT infrastructure that bypasses or contravenes underlying security controls or mechanisms (controls, policies, practices, or procedures) which results in unauthorized access of data, applications, services, computer networks and/or devices. Also the recent US government guides broadly defined breaches in IT security controls to include the loss or theft of devices (e.g., laptops or external drives) and storage media (e.g., disks or USB drives.) (Cate, 2008).

From the above definitions, it is conclusive enough to infer that all activities that result in an unauthorized access of data, applications, services, computer networks and/or devices are classified as breaches in IT Audit controls. Thus, other security challenges such as Bank Impersonation, Cheque Kiting, Forgery and Altered cheques, Accounting Fraud, Identity Theft, Fraudulent Loans, Forged Documents, Fictitious Bank Inspector, Cheque Fraud and Phishing are threats or breaches to IT audit security controls as indicated by (wiseGeek, 2011) and assessed in the sampled financial institutions.

4.4.3 Causes and Effects of Breaches in the IT Control Systems

IT Audit controls' breaches, as outlined by Albrecht et al. (1984) are mainly caused:

i. Having a lot of confidence in employed staff, ii. Improper setup and practices for password verification and validation, iii. Undeclared financial status of organization's personnel iv. Inability to isolate business dealings from caretakers of organization's valuables,

v. Failure to have prudent checks on effectiveness and efficiency, vi. Inability to pay meticulous details to particulars, vii. Inability to isolate organization's valuables from valuable accountability, viii. Inability to have distinctive accountable obligations, ix. Failure to have distinctive lines of administrative controls,

x. Inability to systematically examine systems' reports,

xi. Absence of requirements or conditions for conflicting interest and xii. Inadequate documentations and information

The study carried out in the sampled financial institutions revealed that there was some level of incidence of internal controls' weakness as few cases of unauthorized accesses were recorded in the system log reports. Thus, the above internal weakness, like a small fire outbreak, if not checked would seriously lure the banks to the other security challenges such as Bank Impersonation, Cheque Kiting, Forgery and Altered cheques, Accounting Fraud, Identity Theft, Fraudulent Loans, Forged Documents, Fictitious Bank Inspector, Cheque Fraud and Phishing, as 78 percent of the respondents responded 'YES' to the dangers these security challenges pose to the financial institutions when assessed in the study.

4.5 Internal Auditors' Auditable Roles and Functions

Various Interviews with Internal Auditors made so clear the importance of the Internal Auditors inputs in computerized financial institutions. Their major auditable roles such

as viewing the list of users of the system on daily basis, viewing list of active users at any given time, viewing users records, checking log of user activities, checking exception reports, checking of Assets and Liability report, checking of Internal Account Balances, checking of Suspense Account and General Ledger Account are so technical that these roles have to be done by the Auditors.

The Internal Auditors' sole responsibility of ensuring that a manual call-over of all the daily transactions, especially cash deposits and cash withdrawals are done, to ascertain that appropriate accounts are debited or credited is enough to conclude that the IT Audit controls are not full proof or impervious to other vicious activities of human.

Below are some of the screen shots from Internal Auditors' desk.

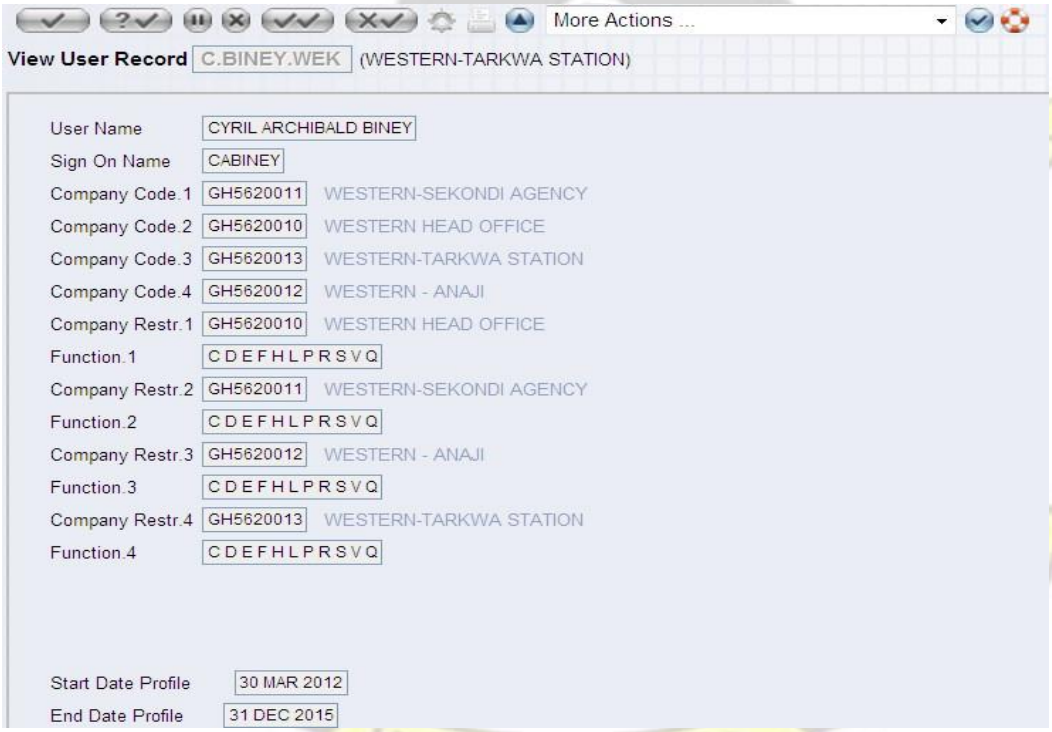


Figure 4.5.1: A User Record being scrutinized by the Internal Auditor

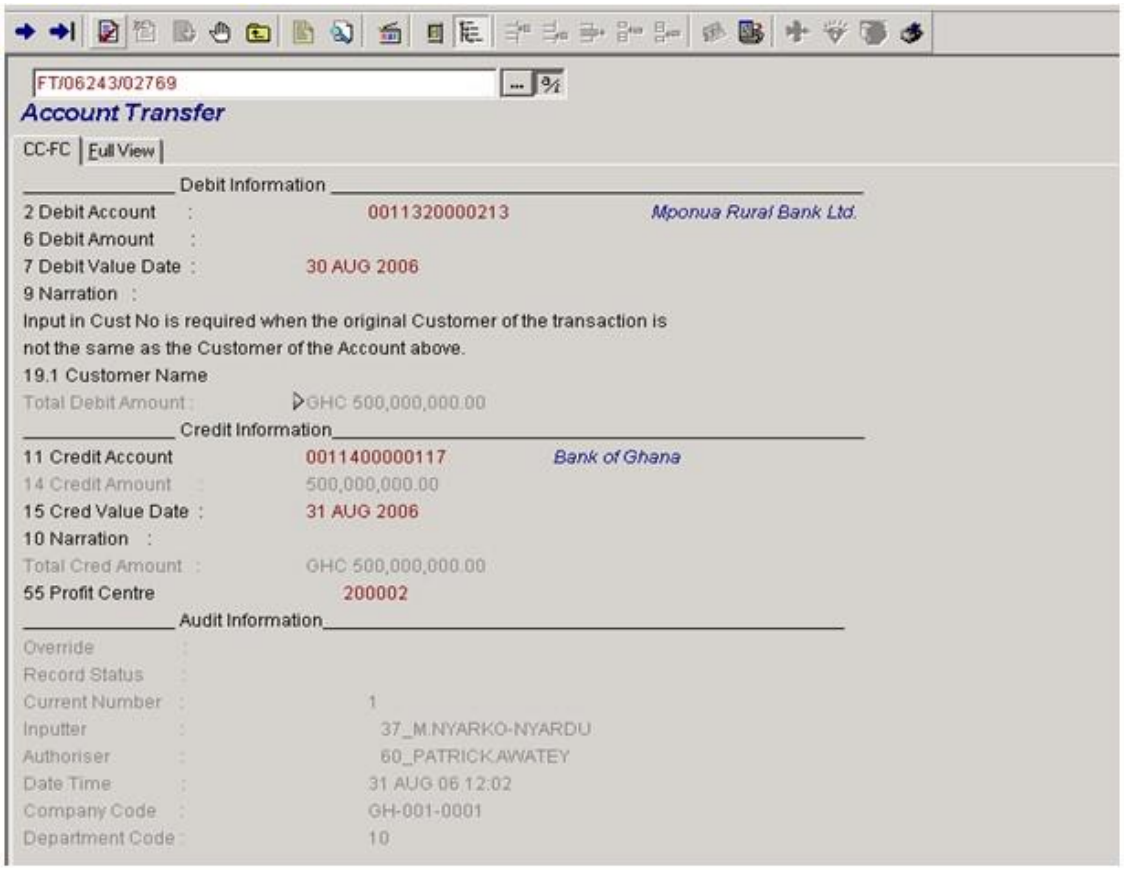


Figure 4.5.2: Funds Transfer Record being reviewed by the Internal Auditor

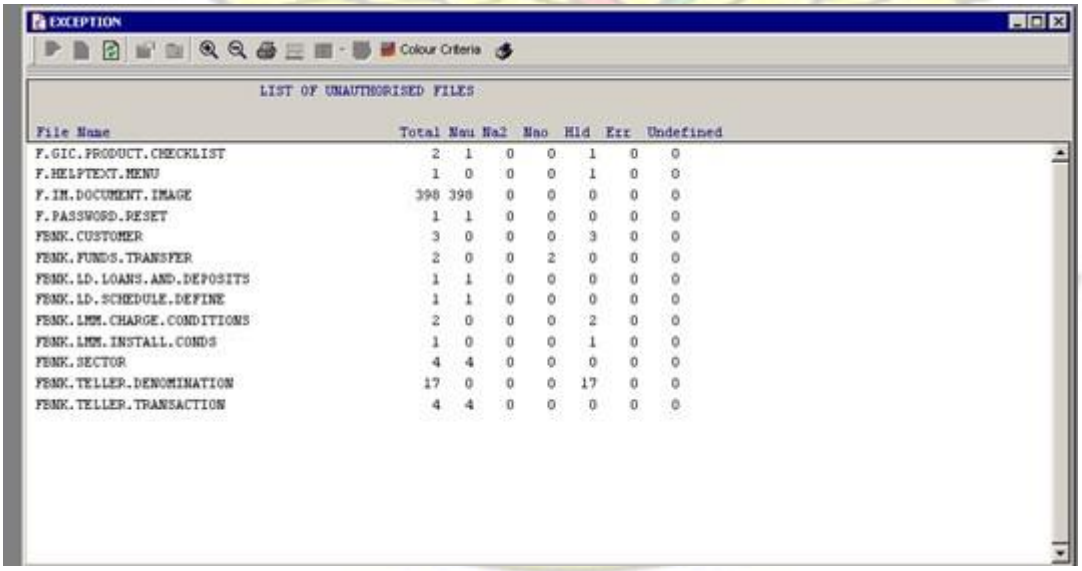


Figure 4.5.3: An Exception Report being reviewed by the Internal Auditor CHAPTER FIVE

CONCLUSION, SUMMARY OF FINDINGS AND RECOMMENDATION

5.1 Conclusion

Information Technology Audit controls in financial institutions has being regarded by financial institutions as an integral part of their business setup. The primary objectives of the research study were to find out the kind of IT Audit controls employed by the computerized financial institutions, to discover some of the likely breaches in the IT Audit controls, the causes and effects of such breaches on the activities of financial institutions and what can be done to maintain or improve the systems in used for effectiveness. A thorough review of the research topic and a statistical analysis of the research were conducted to appreciate the strength and weakness of these IT Audit controls.

5.2 Summary of Findings

Research conducted on the sixteen sampled computerized financial institutions made it very clear that IT Audit controls play very important role in the daily operations of the computerized financial institutions. Conclusively some level of effectiveness of IT Audit controls have been realized by the banks. Hence, the high patronage and high reliance on these IT audit controls by the financial institutions.

The commonly used IT Audit controls are Access Controls, Monitoring Controls, Asset Identification Controls, Asset and Identification Management Controls, Backup and Recovery Controls, Disaster Recovery Controls, Program Change Controls, Network Controls, Computer Operations Controls. The least used controls are the Internet and E-Commerce Controls, Telecommunication Controls.

However, in spite of the IT audit controls existence there were few cases of unauthorized accesses as revealed by the system log reports. Besides, all the sampled financial institutions helplessly admitted to the dangers posed by breaches or other security challenges such as Bank Impersonation, Cheque Kiting, Forgery and Altered Cheques,

Accounting Fraud, Identity Theft, Fraudulent Loans, Forged Documents, Fictitious Bank Inspector, Cheque Fraud and Phishing.

By research, the causes of the above security challenges or breaches were mainly by internal control weakness as outlined by Albrecht et al. (1984). The incidence of some level of internal control weakness recorded during the study was the main cause of few cases of unauthorized accesses captured by the system log repots. Moreover, the daily call-overs by the Internal Auditors to ensure that the appropriate accounts are credited or debited is conclusive enough that IT Audit controls are not full proof or hundred percent dependable.

5.3 Recommendation

"Without audit, no accountability; without accountability, no control; without control, no efficiency; without efficiency, no development" (Daniel, 1999).

The above underscores the need to cost effectively employ more of these IT Audit controls in the day-to-day operations of the financial institutions in the country. Also, for optimum effectiveness, it is not enough to leave the other dimensions of the IT Audit controls (Internet and E-Commerce Controls, Telecommunication Controls and Database Control) untapped, considering the globalization of the computerized technology.

The computerized financial institutions should also pay every price to strengthen the internal controls' systems to safeguard against avoidable IT Audit controls' breaches and other potential security challenges that can break down the financial institutions eventually. Internal Auditors should be encouraged to do more of the manual call-overs of daily transactions since IT Audit controls cannot be effectively relied upon to ensure that appropriate accounts are credited or debited by the inputters.

5.4 Suggested future work

Further research must be undertaken to investigate the recent spate of global internet fraud on credit and debit cards of customers who patronize electronic commerce.

KNUST

REFERENCES

Adam, L. (2013). The Identity Theft Flu: 5 Ways to Keep Yourself Healthy. http://abcnews.go.com/Business/identity-theft-flu-ways-healthy/story?id=19403749. Assessed on 02/11/2013.

Albrecht, W.S.; Howe, K.R.; Romney, M.B. (1984): Deterring Fraud: The Internal Auditor's Perspective. Institute of Internal Auditors Research Foundation, Florida www.uhu.es/ijdar/10.4192/1577-8517-v9_1.pdf. Assessed on 02/03/2013.

Al-Twaijry, A. A. M.; Brierley, J. A.; Gwilliam, D. R. (2004). The development of internal audit in Saudi Arabia: An Institutional Theory perspective. Critical Perspective on Accounting, 14, 507–531.

Anantha, S. (2002). Auditing general and application controls- Information Systems Control Journal 5, 16-19 htpp://www.sirtech.com.au/wp-content/uploads/2012/.../IS_Audit_Process.pdf.
Assessed on 02/03/2013

ARB (2013). Apex Rural Bank Limited.
http://www.arbapexbank.com/rcbs.php. Assessed on 02/03/2013.
http://www.arbapexbank.com/aboutus.php. Assessed on 02/03/2013.
http://www.arbapexbank.com/function.php. Assessed on 02/11/2013.

Badara, S.; Saidin, S. Z. (2013). Impact of the Effective Internal Control System on the Internal Audit Effectiveness at Local Government Level. Journal of Social and Development Sciences, 4(1), 16–23.
http://www.ifrnd.org/Research%20Papers/S31.pdf. Accessed on 03/09/2014

Bierstaker, J. L.; Burnaby, P.; Thibodeau, J. (2001). The Impact Of Information Technology On The Audit Process: An Assessment Of The State Of The Art And Implications For The Future", Managerial Auditing Journal, Vol. 16 Iss: 3, Pp.159 -

164 http://www.emeraldinsight.com/journals.htm%3Farticleid%3D868500. Accessed on 1/9/2014

Bonsor, K. (2001). Is Your Workplace Tracking Your Computer Activities? http://computer.howstuffworks.com/workplace-surveillance.htm> 10/01/2015

Brian, K. (2014). KrebsOnSecurity-In-depth Security News and Investigation: In Wake Of Confirmed Breach At Home Depot, Banks See Spike In PIN Debit Card Fraud. http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depotbanks-see-spike-in-pin-debit-card-fraud/. Assessed on 02/11/2014.

Bruce, S. (2014). Full Disclosure: The Practice Of Making The Details Of Security Vulnerabilities Public.

BusinessDictionary.com (2014). IT security controls' breach. http://www.businessdictionary.com/definition/security-breach.html. Assessed on 02/11/2014.

Bryman, A. and Bell, E. (2003). Business Research Methods. New York: Oxford University Press Inc.

http://www.zdnet.com/meet-the-team/us/charlie-osborne/. Assessed on 02/11/2014.

Cate F.H, (2008). Information Security Breaches, Looking Back & Thinking Ahead http://www.hunton.com/files/Publication/5ad823e3-6eee-45e2-8366-099d431ce4fe/Information_Security_Breaches_Cate.pdf .Assesed on 3/9/2013 **Daniel, E. (1999).** Provision of electronic banking in the UK and the Republic of Ireland. International Journal of Bank Marketing, 17(2), 72-82. http://www.iiste.org/Journals/index.php/RJFA/article/viewFile/7789/8138. Assessed on 02/11/2014.

Eshel, P.; Moore, B.; Shalev, S. (2014). A Changing Battle Space: Prevention Is Not Enough http://techcrunch.com/contributor/shiran-shalev/. Assessed on 03/03/2014

Gary, H. (2008). Putting Security Into IT-Frequently Avoided Questions About IT Auditing http://www.isect.com/html/ca_faq.html-ISECT 2008. Assessed on 02/11/2014. http://www.isect.com/IsecT_IT_Audit_FAQ_March_2008.pd. Assessed on 02/11/2014.

Ge, W., McVay, S. (2005). The Disclosure Of Material Weaknesses In Internal Control-After The Sarbanes-Oxley Act. Accounting Horizons 19, 137–158 https://zicklin.baruch.cuny.edu/centers/zcci/downloads/determinants-of-weaknesses-ininternal-control.pdf. Assessed on 02/02/2015.

Goldberg, D. M. (2011). General Auditing for IT Auditors. ISACA Journal, 3, 1–4. http://www.isaca.org/Journal/archives/2011/Volume-3/Pages/General-Auditing-for-IT-Auditors.aspx-ISACA- Accessed on 1/9/2013

Hayale, T. H.; Khadra, A. A. H. (2006). Evaluation of The Effectiveness of Control Systems in Computerized Accounting Information Systems : An Empirical Research Applied on Jordanian Banking Sector. Journal of Accounting – Business & Management, 13, 39–68. **iREACH, (2013)**. 2012 Sets New Record for Reported Data Breaches http://www.ireachcontent.com/news-releases/2012-sets-new-record-for-reported-databreaches-191272781.html. Accessed on 1/9/2014

INTOSAI (2014). Information Technology Audit-IT Audit Monograph Series # 1 (http://intosaiitaudit.org/India_GeneralPrinciples, 2010). Assessed on 3/9/2014

ISACA (2011). General Auditing for IT Auditors http://www.isaca.org/Journal/archives/2011/Volume-3/Pages/General-Auditing-for-IT-Auditors.aspx-ISACA-**Assessed on 1/9/2013**

Javelin, S.; Research (2013). Identity Theft Fraud:1 In 4 Data Breach Notification Recipients Become A Victim Of Identity Fraud. https://businessadvocate.mcdonaldhopkins.com/community/protecting-yourbusiness/data-privacy/blog/2013/11. Assessed on 02/11/2014. **Kenneth, M. (2010).** IT Auditing and Controls: An Introduction http://resources.infosecinstitute.com/it-audit-

introduction/. Assessed on 02/11/2014. **Levine, M. H. (2013).** Proposed IT Audit Scope To Support: The Annual Financial

Statement Audit.

http://www.psc.gov.za/documents/2013/Annual%2520report%2520201213.pdf. Accessed on 3/9/2014

https://www.javelinstrategy.com/brochure/276#DownloadReport. Accessed on 3/9/2013

Margaret, R. (2010), WhatIs.com, TechTarget's IT Encyclopedia And Learning Center http://searchsecurity.techtarget.com/definition/data-breach. Assessed on 02/11/2014. http://www.techtarget.com/contributor/Margaret-Rouse. Assessed on 02/11/2014. **Malhotra, K. N. (2007).** Research Design and Methodology http://shodhganga.inflibnet.ac.in/bitstream/10603/6582/13/13_chapter4.pdf **Microsoft (2012).** The Event and Transaction Logs http://windows.microsoft.com/en-us/windows/what-information-event-logs-eventviewer#1TC=windows-7. Assessed on 02/09/2014. http://windows.microsoft.com/en-us/windows/what-information-event-logs-eventviewer#1TC=windows-7. Accessed on 03/09/2014

Musa, A. A. (2004). Investigating the Security Controls of CAIS in an Emerging Economy: An Empirical Study on the Egyptian Banking Industry. Managerial Auditing Journal, 19(2).

Okonji. E. (2014). Banks Find Succor in Temenos T24 Banking Solution Software http://www.thisdaylive.com/articles/banks-find-succor-in-temenos-t24-bankingsolution-software/171269/. Assessed on 02/11/2014.

Osborne, C. (2014). Between The Lines. TC News Letter

Pathak, J. (2009). IT Auditing and Electronic Funds Transfers. JEL, 18(5).

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=623585. Accessed on 03/09/2014

PCAOB, (2007). Auditing Standards

http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard

PROTIVITI, (2009). IT General Controls

http://www.asu.edu/fs/documents/icq/IT_general_controls_icq.pdf. Assessed on

03/09/2014

http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/QuestionnairesITGeneralControls!OpenDocument-. Assessed on 03/09/2014

Rainer, R.; Kelly, and Casey G. C. (2011). Introduction To Information Systems. 3rd ed. Hoboken, N.J.: Wiley

Reuters (2014). 'Home Depot confirms security breach following Target data theft'. Home Depot Inc http://www.reuters.com/subjects/top-100-global-innovators?ic=int_mb_100. Assessed 03/09/2014

Robson, C. (2002). Real world research: A resource for social scientists and practitionerresearchers (2nd ed.). Oxford, UK: Blackwell

Singleton, T.W. (2008). What Every IT Auditor Should Know About Access Controls http://www.isaca.org/Journal/Past-Issues/2014/Pages/default.aspx. Assessed

03/09/2014

Temenos, G. (2012). Temenos T24 product overview.

www.e-incube.com/downloads/**TEMENOS_Product**_Brochure.pdf

http://www.booksu.net/pdf/title/temenos-t24.html. Assessed on 03/09/2013

http://www.search-document.com/pdf/1/temenos-architecture.html. Assessed on

03/09/2013

Vangie, B. (2014). Audit trail http://www.webopedia.com/TERM/A/audit_trail.html. Assessed 03/11/2014 http://www.webopedia.com/Author/Vangie-Beal. Assessed 03/11/2014 **wiseGeek, (2011).** Bank Fraud http://www.wisegeek.com/-Assessed on 03/10/2013 http://www.iiste.org/Journals/index.php/RJFA/article/viewFile/7789/8138. Assessed on
03/10/2013

KNUST

ZAK, S. (2014). The War With No End
https://www.internetretailer.com/2014/09/02/war-no-end. Assessed 03/11/2014
http://www-csag.ucsd.edu/projects/Optiputer/papers. Assessed on 03/11/2014
http://www.isaca.org/Journal/Past-Issues/2002/Volume-5/Pages/Auditing-General-andApplication-Controls.aspx) Assessed on 03/11/2014

APPENDICES

APPENDIX I: SAMPLE QUESTIONNAIRE FOR FINANCIAL INSTITUTIONS' MANAGEMENT STAFF

KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

INSTITUTE OF DISTANCE LEARNING

RESEARCH QUESTIONNAIRE

This questionnaire seeks to collect data for a research study on **"Investigating the Effectiveness of Information technology Audit Controls In Financial Institutions"**

PREAMBLE

IT Audit controls are distinctive setups and procedures that are electronically defined by institutions to effectively and efficiently bring to pass the realization of the institutions' objectives and set goals. The objectives of these distinctive setups and procedures also focus on sensitivity, wholeness, and accessibility of data and the entire management of the information technology setup, (PCAOB, 2007).

KNUST

Thank you.

QUESTIONNAIRE ON INVESTIGATING THE EFFECTIVENESS OF (IT) AUDIT CONTROLS IN FINANCIAL INSTITUTIONS

Name of Bank…….....…….Position/Office……
Location……..Region……

SN	QUESTIONS (Please indicate by ticking the option that best suits the question)	TICK
	Demographic Characteristics	
1	**Gender:**	
	Male	
	Female	
2	**Age Group**	
	18 – 25 years	
	26 - 30 years	
	31 – 35 years	
	36 – 40 years	
	More than 40 years	
3	**Educational Level (indicate as many as apply)**	
	Senior high School	

	Tertiary or Higher Education		
	Other:		
4	**Field of Study (indicate as ,many as apply)**		
	Business Related		
	Science Related		
	Computer Related		
	Other:		
5	**Does the Bank use the following controls in ensuring that its business objectives are met? (Please thick Yes or No where appropriate)**	**YES**	**NO**
a	**Access controls –** (physical and logical controls using software and data to monitor and control access to information and computer systems)		
b	**Monitoring Control –** (event information that will be logged and monitored and alert levels that will be triggered for incident response)		
c	**Asset Identification Controls** (operational procedures related to asset inventory, accountability, responsibility and information classification)		
d	**Asset and Identity Management Controls** (hiring, termination and background checking procedures for the organization's workforce members)		
e	**Backup and Recovery Controls? (**Provisions to provide reasonable assurance that an organization will be able to recover from loss or destruction of data processing facilities, hardware, software or data		

f	**Disaster Recovery Controls?**		
g	**Program Change Controls?**		
h	**Network Controls**		
i	**Computer operations Controls?**		
j	**Internet and E – commerce Controls**		
k	**Telecommunication Controls**		
l	**Database Controls?**		
6	**What accounting software does the bank use?**		
7	**Do you have a specific user password with which you access your PC electronically?**		
8	**Does your specific user password get expired?**		
9	**Have you had occasions where other staff gained electronic access to your working PC without your prior permission?**		

KNUST

a	If yes, were you alarmed?		
b	What were your fears? ……		
c	What led to such an unauthorized access to your working PC? …….		
10	**Has there been any occasion where auditors (internal or external) or an officer suspected a crime as a result of a breach in IT controls?**		
a	If yes, what was the crime? ……..		
b	If yes, what caused it? …….		

KNUST

TO WHAT EXTENT DO YOU AGREE ON THE FOLLOWING? PLEASE INDICATE YOUR OPINION BY TICKING THE APPROPRIATE OPTION						
	Question on Access Controls	**AGREE**	**STRONGLY AGREE**	**DISAGREE**	**STRONGLY DISAGREE**	**NOT SURE**
11	**The Bank IT audit controls include unique password**					
12	**The IT audit controls include passwords change on a periodic basis**					
13	**The IT audit controls includes cancellation or access rights modification upon an employee's termination or transfer in a timely manner**					
14	**System generated reports are regularly reviewed by the security administrator**					
15	**The system generated reports are able to show authorized and unauthorized access to the banking software**					
16	**Procedures are in place to follow up on these system generated reports**					
17	**IT audit control systems are set up to safeguard institution's operation against perceived threats or impending dangers**					
18	**Shareholders of the Bank have absolute confidence in the system security offered by the IT audit controls?**					

19	**System users have absolute confidence in the system security offered by the IT audit controls**					
20	**Banking customers have absolute confidence in the security of the computerized system being used to serve them**					
21	**Do you share the view that computerized banking software has contributed greatly to reduce banking crimes or frauds**					
22	**There are still security challenges in spite of the IT audit security control**					
	systems being used.					
23	**Some of the security challenges are:**					
a	Bank impersonation					
b	Cheque Kiting					
c	Forgery & Altered Cheques					
d	Accounting Fraud					
e	Identity Theft					
f	Fraudulent Loans					
g	Forged document					
h	The Fictitious bank inspector					
i	Cheque Fraud					
j	Phishing					

KNUST

APPENDIX II: SAMPLE INTERVIEW QUESTIONS FOR FINANCIAL INSTITUTIONS' MANAGEMENT STAFF

INTERVIEW GUIDE FOR GATHERING DATA ON

EFFECTIVENESS OF IT AUDIT CONTROLS IN FINANCIAL INSTITUTIONS

QUESTIONS

1. Apart from the Bank Manager what are the other positions held by other officers in your institution?.....
2. Has the Bank computerized all its operations?.....
3. Does the Bank use any computerized software?.....
4. Is the institution affiliated to ARB Apex Bank?.....
5. What are the main functions of the system Administrators?.....
6. What are the main functions of the Internal Auditor?.....
7. Apart from the System Administrator what are other category of users hooked to the computerized system?.....
8. Functions of other users attached to the computerized system?.....
9. Any available institutional hardcopy documents for the purpose of my study?.....
10. What are the various IT Audit controls used to safeguard daily operations?.....