THE IMPACT OF INFORMATION TECHNOLOGY ON AUDIT PRACTICE: THE CASE OF

UNION SAVINGS AND LOANS COMPANY LIMITED

KNUST

BY

JESSE KYEI PEPRAH (BSc. Business Administration)

A THESIS SUBMITTED TO THE INSTITUTE OF DISTANCE LEARNING, KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY IN PARTIAL FUFILMENT OF THE REQUIREMENT FOR AN AWARD OF COMMONWEALTH ÞXECUTIVE MASTERS DEGREE IN BUSINESS ADMINISTRATION.

JUNE, 2013

DECLARATION

I hereby declare that the submission of this compilation is the true findings of my own researched work presented towards an award of a second degree in the Common wealth Executive Masters in Business Administration and that, to the best of my knowledge, it contains no material previously published by another person nor submitted to any other University or institution for the award of degree except where due acknowledgement has been made in text .However, references from the work of others have been clearly stated.

Jesse Kyei Peprah (PG6399511) .... June 2013

Student Name & ID **Signature** **Date**

Certified by:

Dr. C.K Osei ....

Supervisor's Name **Signature** **Date**

Certified by:

Prof. I. K. Dontwi .... [illegible]

Dean IDL **Signature** **Date**

DEDICATION

I dedicate this book to my parents Mr.& Mrs Kyei Peprah for their support, to all my lecturers and colleagues who with their support help make my days in school very successful and to all those who directly or indirectly contributed to the success of this book.

ABSTRACT

The effective use of information Technology (IT) has the potential to yield significant benefits in the financial Industry. The main objective of this study is to evaluate the impact use of IT in a financial institution in Ghana. The study population consisted of the internal auditors, external auditors, IT technicians at Union Savings and Loans (USL). Cross sectional survey design was used. Both primary and secondary data were gathered for the study. Data were collected using questionnaires and interviews. The target population for this study consisted of all the staff of Union Savings and Loans Ltd. A systematic sampling method was used to select the auditors' staff and IT technicians of the USL in all the branches in Ghana. The study reveals that the majority of the respondents were of the

KNUST

IT policy of USL; however the level of understanding of the staff on IT policy was mixed. Generally, most of the respondents used IT in their field operations. The study reveals that training in IT skills was inadequate. The respondents believed that having adequate skills in advance excel and access could improve the performance of their work. The challenges the respondents faced in the use of IT tools at USL include the absence of dependable network connections, frequent power outages and the delays due to supply of PCs and accessories. In terms of effectiveness of IT on the operations of USL, majority of the respondents stated the use of IT was more effective on the detection of fraud and error than the manual process. Improving the use of IT at USL will require the acquisition of modern IT equipments, provision of computers; proper network connections in all offices, proper supervision, and regular review of the IT policy at the company.

TABLE OF CONTENT

KNUST

CONTENTS

KNUST

KNUST

KNUST
NYANSAPO WO SANE NO BADWENMA

CHAPTER ONE

1.1 Background of the study:

Information has become a commodity that has value, which is bought and sold. With the increased importance that information has gained, there is the need to create a support for activities involving the gathering, storing, processing and communication of information. This is the role that Information Technology has come to play. However, information technology does not operate in a vacuum but operates through a set of connected processes and procedures for handling information which is termed as an Information system. An information system consists of a data processing installation, a database and programs for evaluating the data. Examples of information Systems are Management Information Systems, (Transactional Processing Systems, Knowledge Working Systems, Decision Support Systems, and Expert Support Systems). Therefore, Information Technology may be seen as the broadly based technology needed to support information systems.

In the early days, computers were developed to provide solutions to specific problems. Now, the commercial business computer is a general-purpose programmable device capable of supporting many applications designed to meet the needs of a whole organization. All enterprise now has at least accounting records on a computer but there are few organizations that do not rely, to some extent, on information technology. With the advent of inexpensive microcomputer systems, even the smallest audit clients are likely to use computer for many accounting functions. This having a great impact on —auditing and auditors must be prepared to work in an ever-changing environment in which the clients accounting records are maintained as anything from a personal computers to a multimillion dollar one.

Electronic service thrives with Information Technology and is becoming increasingly important not only in determining the success or failure of electronic commerce, but also in providing consumer with respect to the interactive flow of information. The technological development in the financial industry in Ghana is now rampant and almost every financial institution within the industry has one way or the other using Information Technology to serve it client. This makes it imperative to incorporate Information Technology in Auditing the financial Industry.

1.2 Problem Statement

While the impact of information technology (IT) in the business world has grown exponentially in the past two decades, few studies have examined audit IT usage and the perceived importance of IT usage, particularly outside of the largest audit firms (Fischer 1996; Banker et al 2002). This is an important issue since IT has dramatically changed in the audit process and may be potential barrier to entry in public accounting. Standards now encourage audit firms to adopt IT and use IT specialist when necessary (AICP 2001, 2002b, 2005, 2006b: PCAOB 2006b). Auditing researchers and practitioners have little guidance available on what IT has been, or should be adopted by auditing firms. Concerns have raised that smaller financial institution may not be able to compete with larger firms on IT investments in auditing resulting in potential economic barriers to entry as well as audit effectiveness and efficiency issues (POB 2000; GAO 2003). Furthermore, previous researches have not addressed the extent to which second tier or national firms have utilized IT application, despite the fact that these firms have many Security and Exchange clients (International Accounting Bulletin 2005).

Situation in Ghana in this respect is not much different, in the Governor of Bank of Ghana address at —the annual dinner of the chartered institution of bankers and financial institutions on 27th November 2010 with the theme challenges to the Ghanaian economy, Mr Kwesi Bekoe Amissah — Aurthur acknowledges that the pace ofIT usage in the financial industry requires continuous knowledge update by both operators and regulators (Auditors), this is as a result of the global financial crisis. He further emphasize that operational risk has assumed great reliance on information technology or IT platforms

LIBRARY
KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY

for the delivery of financial services, this has made it necessary for the need of regulators to acquire special expertise in IT auditing to ensure appropriate monitoring of IT related vulnerabilities in the financial industry he concludes and further assures that the Bank of Ghana will insist on all stakeholders in the industry to improve their corporate governance systems, especially the installation of an effective internal control systems

KNUST

This study therefore, sought to examine the role of Information Technology in the Financial Industry and analyze appreciably the challenge that traditional audit practice (which is mostly manual) in the Financial Industry face and how the IT audit dynamic innovation does effectively rectify it. The investigation will outline the human factor of resistance to any change, as well as the readiness of the Auditors to inculcate the changes into their operations. The relevance of IT Audit and the dynamism that it brings coupled with the human resistance factor to changes in an organization constitute the major hurdles that a dynamic innovation company has contended with. These will however be analyze by the study to reveal their positive impact or otherwise.

1.3 Research Objectives

The main objective of this research is to examine the impact of the Information Technology in the Audit Practice in Union Savings and loans, Ghana. The specific objectives of this project include:

1. To find out the effect of information technology on audit procedures in the provision of services in the financial industry.
2. To ascertain how information technology has facilitated the detection and minimization of the occurrence of fraud and error in the Savings and Loans sector
3. To examine Auditors reaction to new technology.
4. To investigate the challenges associated with the use of IT in Audit procedures in the financial Industry

1.4 Research Questions and Hypothesis:

1. To what extent has IT affected audit procedures in Union Savings and Loans Company Limited?
2. To what extent has IT facilitated the detection and minimization of occurrence of fraud and error in the financial institution?
3. What is the reaction of auditors to new technology change in the financial institution?
4. What are the problems relating to the use of IT in Audit procedures in the financial Industry?

1.5 Relevance of the Study:

The modern business environment requires business to adapt to ever-changing environment conditions. This research will examine in detail the issues surrounding the implementation of a new audit information system, which will identify major problem areas when implementing information system. This research will show light into the problems associated with the ordinary auditing procedures as compared with that of the IT auditing (and its implementation), which will encourage others to conduct further research to find solutions to some of the problems that will be revealed in this research project. Moreover, it will provide background information to auditors, the Financial Industry and the Ghanaian economy as tú-<Gåiting procedures are carried out in an economic, effective and efficient manner. In addition, it will encourage organizations and other Financial Institution who are not using IT to adopt the use of IT in the daily operations of their businesses, to enable them to be highly competitive.

1.6 Scope/Limitation of the Study:

Bank of Ghana policies and regulations on Auditing of Financial institution states that all financial institutions should have both internal and external auditors. The study will be undertaken mainly base on the internal and external auditors of Union Savings and loans and their staffs. The internal auditors

KNUST

are under their internal control department while their external auditors are Charles Allotey & Co Ltd which is an Auditing Firm.

There are four main challenges that the researcher expect to encounter. They are:

I. Finance- Money to finance transportation, typing, printing, binding and photocopying

Il. Time- much time needed to gather information from the media, distribute and collect questionnaire, see the supervisor for direction and correction, analyse data and write the project for submission

Ill. Personnel- acquiring human resource to carry out a task is a great challenge and also to gain attention and willingness of respondents to provide me with information required within a specific period will be a challenge.

IV. The sampling area: Union Savings and Loans and their External Auditors will be the main focus of this research. This will make the size of the sampling area small as compared to that of all the financial institutions and audit firms in Ghana.

1.7 Organization of the thesis:

—This study will be organized in five chapters. Chapter one will be an introductory one and it will consist of the background to the study, statement of problem and research objectives. The review of relevant literature will be presented in chapter two while the research methodology will includes the study area, population sample and research instruments. The analytical presentations and discussion

LIBRARY
KWAME NKRUMAH UNIVERSITY OF

will be outline in chapter four, while chapter five will summarizes the findings and draw conclusions on the findings while providing recommendations on the research conducted.

KNUST

NYANSAPƆ WƆSANE NO BADWENMA

KNUST

CHAPTER TWO

LITERATURE REVIEW

2.0 INTRODUCTION

Millichamp, 2002 discusses that, "Computing or computer information systems are a component of almost all audits". However, it is worth considering how this system has affected auditing. Although it has created a challenging problem to auditors, it has broadened their horizons and expand the range and value of services they offer. The computer is more a tool for performing routine accounting task with unprecedented speed and accuracy. It makes possible the development of information that could not have been gathered in the past because of time and cost limitations when a client maintains accounting records with a complex and sophisticated Electronic Data Processing System (EDPS), auditors often find it helpful and ever necessary to utilize the computer in performing many auditing procedures. Due to the demand of today's computerized environment an auditing manager must possess sufficient knowledge of the computer information to plan direct and review the information processed.

2.1.0 GENEARAL PRINCIPLES

2.1.1 What is IT and Auditing?

Information Technology describes any equipment concerned with the storage, transmission or presentation of information

Automation and rapid IT development are affecting all aspects of life the auditing profession is no exception. The Laptop computer and the Internet have been recruited to assist in auditing, whilst the essential process of the audit is the same the computerized techniques and software available to the auditor has developed significantly.

2.1.2 What is An Audit and it's Objectives?

LIBRARY
KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY

An audit is defined as independent examination and expression of opinion on, the financial statement of an organization, by an appointed auditor in pursuance of that appointment and in compliance with any relevant statutory obligation (www.goldsmithibs.com/freedownloads/Auditing/whatisAuditing.pd.

Financial statements are defined as balance sheet and profit and loss account (or other form of income statement) together with such additional statements and notes as are identified as being within the scope of audit opinion (Auditing Standards and Guidelines, ISSAI 3000).

The primary aim of an audit is to enable the Auditor to form and express an independent and expert opinion on the financial statements. The opinion expressed is usually as to whether or not the Auditor believes that the financial statements present a true and fair view of the financial position of the origination and of its profit or loss for the period under review.

As a basis for the formation of his opinion the Auditor verifies the accuracy of the data being processed in the accounting system prior to its convention into the financial statement under review. Thus the Auditor becomes concerned with the adequacy of the accounting system and the accuracy of the figures in the accounting record. The subsidiary aim of an Audit is to detect and prevent errors and fraud, by the deterrent and moral effect of the Audit and also by assisting client to institute improved financial control (Anand, 201 1).

2.1.4 Types of Audit

Pany Et al, 2004 discusses that the fundamental scope of an IT audit is no different to that of an audit carried out for the same purpose in a non-computerized environment. However, the objectives or scope of the audit will differ with the type of audit being carried out. Financial, value for money, security and forensic Audit are the different types of audits.

In financial audit, the auditor aims to test the integrity of the assertions made by management in the financial statements regarding existence, occurrence, completeness, valuation, rights and obligation concerning ownership, measurement, presentation disclosure and regularity. With this, the auditor therefore confines his work to financial systems (Pany Et al 2004).

KNUST

In value for money audit the auditor aims to test systems as to economy, efficiency and effectiveness and is not confined to financial systems. Security audit is done to test all systems as to their confidentiality, integrity and availability. With this the auditor's objective is to assess whether management have undertaken sufficient work to reduce residual risk to an acceptable level.

Forensic Audit is investigate since the Auditor seeks to explain irregularities, anomalies or fraud through the analysis of systems and stored information.

2.1.5 Who an Auditor and Types of Auditors?

An auditor is a person who reports on the accounts of an organization. His main task is to examine the accounts and the underlying records giving rise to entries therein and report whether in his opinion they properly reflect the activities of the organization during the period under consideration and of its assets and liabilities at the end of that period. In reality, although auditors use the singular form, Auditing firms do not describe themselves as auditors, but they rather describe themselves as Chattered Accountants (e.g. Ayew Agyeman Turkson and co.) or accountants. Even small firms especiallbperform othep-sõïðêš-šÛch as writing up and balancing books, preparing final accounts, tax negotiations, financial advice, management and system advice, liquidation and receivership work etc. mostly one or more of those partners is responsible for the conduct ofthe audit and the singing of the report on behalf of the firm (Kumar Et al, 2005).

Auditors may be categorized as Internal Auditors and External Auditors. The particular audience to which each presents their audit opinion can define the distinction between the two.

KNUST

The work of an Internal Auditor is defined as the functional means by which the managers of an entity receive an assurance from internal sources that the process for which they are accountable are operating in a manner which will minimize the probability of the occurrence of fraud, error or inefficient and uneconomic practices. They therefore report to the management of an entity and are often involved in a system development and management service (Pickett, 2004).

The work of an external auditor is aimed at providing an independent opinion as to the probity of financial statement for the benefits of the owners of an entity and not on behalf of management. It is known that accounts will not be true and fair unless the information they contain is sufficient in quantity and quality to satisfy the reasonable expectations of readers to whom they are addressed.

According to Millichamp, 2002 IT Audit is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organizational goals to be achieved effectively, and uses resources efficiently. Data integrity relates to the accuracy and completeness of information as well as to its validity in accordance with the norms. An effective information system leads the organization to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives. IT Auditor

must knovvthe he characteristics of users of the information system and the decision-making environment

in the audited organization while evaluating the effectiveness of any system. Use of computer facilities has brought radically different ways of processing, recording and controlling information and has combined many previously separated functions.

KNUST

The potential for material systems error has thereby been greatly increased causing great cost to the organization, e.g., the highly repetitive nature of many computer applications means that small errors may lead to large losses. An error in the calculation of Income Tax to be paid by employees in a manual system will not occur in each case but once an error is introduced in a computer system, it will affect each case. A Financial institution may suffer huge losses on account of an error of rounding off to next cedis instead of nearest pesewas. This makes it imperative for the auditor to test the invisible processes, and to identify the vulnerability in a computer information system as the costs involved, because of errors and irregularities, can be high.

As computer technology has advanced, government organizations have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. As a consequence, the reliability of computerized data and of the system that process, maintain and report these are a major concern to audit. IT Auditors evaluate the reliability of computer-generated data supporting financial statements and analyse specific programs and their outcomes. In addition, IT Auditors examine the adequacy of controls in information systems and related operations to ensure system effectiveness.

2.2 Control in a Computer system

Computer systems are efficient and achieve results accurately and at great speed if they work the way they are designedto. They have controls provided to ensure this but the controls have to be effective. The controls are of great value in any computerized system and it is an important task for an auditor to see that not only adequate controls exist, but that they also work effectively to ensure results and achieve objectives. Also controls should be commensurate with the risk assessed so as to reduce the impact of identified risks to acceptable levels (Spanos Et al, 2001).

KNUST

Controls in a computer information system reflect the policies, procedures, practices and organizational structures designed to provide reasonable assurance that objectives will be achieved. The controls in a computer system ensure effectiveness and efficiency of operations, reliability of financial reporting and compliance with the rules and regulations.

Information system controls are broadly classified into two broad categories:

- General Controls
- Application controls

General controls include controls over data centre operations, system software acquisition and maintenance, access security, and application system development and maintenance. They create the environment in which the application systems and applications control operate. Examples include IT polices, standards, and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, service continuity planning, IT project management, etc (Spanos Et al, 2001).

Application controls pertain to specific computer applications. They include controls that help to ensure the proper authorization, completeness, accuracy, and validity of transactions, maintenance, and other types of data input. Examples include system edit checks of the format of entered data to help prevenVÞssible invalid input, system enforced transaction control that prevent users from

performing transactions that are not part of their normal duties, and the creation of detailed reports and —transaction control totals that can be balanced by various units to the source data to ensure all transactions have been posted completely and accurately.

2.3 Significance and Objectives of Controls

According to Spanos Et al, 2001, the presence of controls in a computerized system is significant from the audit point of view as these may allow duplication of input or processing, conceal or make invisible some of the processes, and in some of the audited organizations where the computer systems are operated by outside contractors employing their own standards and controls, making these system vulnerable to remote and unauthorized access. Apart from this, the significance of controls lies in following possibilities:

i) Data loss due to file damage, data corruption (manipulation), fire, burglary, power failure (or fluctuations), viruses etc

ii)Error in software can cause manifold damage as one transaction in a computer system may affect data everywhere; iii) Computer abuse like fraud, vengeance, negligent use etc. is a great potential danger and iv) Absences of audit trails make it difficult for an auditor to ensure efficient and effective functioning of a computerized system.

The objectives of controls do not change with the introduction of computers. It is the control techniques that change with many of the manual controls being computerized and new technical computer controls added to achieve the same objectives. Typical control objectives within a government Data Processing function to ensure:

i.Provision of effective organizational control over functions related to Data Processing by clearly defining organizational objectives; ii. Effective management control over development of Data Processing resources in accordance with organizational objectives;

iii. Practices related to Data Processing activities in accordance with statutory requirements and down administrative procedures;

KNUST

iv. Formulation of an adherence to policies, standards and procedures for all functions related to Data Processing and

v. Efficiency and effectiveness of the Data Processing systems towards achievement of its desired objectives.

2.5 Preliminary Evaluation

The first step in audit should be preliminary evaluation of the computer systems covering:

i. How the computer function is organized ii. Use of computer hardware and software, iii. Applications processed by the computer and their relative significance to the organization iv. Methods and procedures laid down for implementation of new applications or revision to existing applications. In course of preliminary evaluation, the auditor should ascertain the level of control awareness in the audittee Organization and existence (or non-existence) of control standards. The preliminary evaluation should inter alia identify potential key controls and any serious key control weaknesses. For each control objective the auditor should state whether or not the objective has been achieved; if not, he should assess the significance and risks in ed with due to control deficiencies.

2.6 Audit Methodology

After completing the preliminary evaluation of the computer systems, the auditors have to decide about the appropriate audit approach system based on direct substantive testing. In doing so, the aspects to be borne in mind are (Anand, 2011):

i. Results of the preliminary evaluation ii. Extent to which reliance can be placed on any work carried out by Internal Audit iii. Nature of any constrains like lack of any audit trail and the practicability of testing.

iv. Effective compliance testing of key computer controls (which may be difficult) and

v.Each control to be tested will require large samples.

2.6.1 A direct substantive Testing

If direct substantive Testing approach is chosen, a sample of transactions should be selected and tested. Result of the preliminary evaluation will be of help particularly as it would have:

i. Provided an overall assessment of the control environment and identified any serious ii. Weaknesses which should be raised with the auditee, iii. Given sufficient familiarity with the system to be able to decide the point from which to select the transactions for testing and how to substantiate them efficiently and iv. Provide sufficient information to determine any initial requirement for any Computer assisted audit techniques (CAATs).

2.6.2 System Based Audit

For system Based audit approach, aspects of regularity, economy, efficiency and effectiveness of the system have to be looked into besides evaluating data integrity, and data security as explained below:

i) System effectiveness is measured by determining whether the system performs the intended functions and whether users get the needed information, in the right form when required;

KNUST

LIBRARY

ii) A system is economical and efficient if it uses the minimum number of information resources to achieve the output required by the users. The use of system resources –hardware, software, personnel and money — should be optimized; iii) System activities would be regular if they comply with

KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY

applicable laws, rules, policies, guidelines, etc iv) Achieving data integrity implies that the internal controls must be adequate to ensure that errors are not introduced when entering, communicating, processing, storing or reporting data; and

v) Data system resources, like other assets, must be sufficiently protected against theft, waste, fraud, unauthorized use and natural disasters.

The key controls for ensuring the above will have to be identified, recorded, and evaluated and compliance tested. The result of the preliminary evaluation would be of help particularly as they would indicate system deficiencies, major weaknesses and the areas requiring in-depth study. Identification of key controls would also depend on experience of the auditor gained in course of audit of similar installations. Compliance testing of controls in computer systems and programmes is difficult and complicated as their operation is automatic, invisible and not fully evidenced (only the exceptions are normally evidenced). Detailed manual testing of these controls is rarely cost effective, but a possible alternative approach is to use a CAATS.

For example, either test data or audit software may be used to test a control, which is designed to -ensure that payments exceeding a certain value should not be made. Audit software can be used to interrogate the whole payments file to identify any payments, which exceeded the specified value. If no such cases are revealed, theauditor has some, assurance in that no such payment was made. This is a negative assurance since it is possible that no invalid data was in fact presented to the system (and hence the control was never invoked). However, if the interrogation is applied to the whole year's transactions, it achieves the main audit objective in that no excessive payments will have been made in the period. Even when test packs or interrogation are used, the auditor should examine the procedures for dealing with exception or error reports, to ensure that invalid transactions are corrected and reinput for processing.

2.7 Audit Techniques

Basu, 2006 discusses that IT audit techniques refer to the use of computers, including software, as a tool to independently test computer data of audit interest. Some well-established techniques are:

i.Collecting and processing a set of test data that reflects all the variants of data and errors which can arise in an application system at different times; ii. Using integrated test facilities, built into the system by the auditee to help the auditor in his requirements, as one of the users of the system; iii. Simulating the auditee's application programs using audit software to verify the results of processing;

iv.Reviewing program listings periodically to see that there are no unauthorized alterations to the programs;

v.Using either commercial software or in-house developed programs to interrogate and retrieve data applyin sele •on criteria and to perform calculations and vi. Extracting samples of data from the auditee database/ files, using sampling techniques, for post analysis and review. The nature of data and type of analysis required determine what technique is to be employed. The auditor should give the sample size and design.

LIBRARY
KWAME NKRUMAH UNIVERSITY OF

2.7.1 Computer audit techniques are employed for:

i. Verification of ledger balances and control totals independently ii. Recalculation of critical computerized calculations to check mathematical correctness; iii. Range checks to verify the working of computer based controls and testing for exception conditions; iv. Testing the validity of data which have gone into the master file

v. Detection of data abuse/ frauds and vi. Substantive testing with large volumes of data which is difficult, if not impossible, in a manual audit process.

2.7.2 The particular computer audit technique employed depends on:

i.The type of application system under review; ii. The extent of testing required; iii. The availability of resources in terms of computer facilities, and the level of EDP skills among the audit staff; and iv. Volume of data and availability of printer information. Where data volume is small and adequate printed information is available to carry out a meaningful clerical and time consuming. To elaborate further, the auditor should break up his project of application system audit into three stages. In the first stage, he will carry out the examination of audit trails,

intermediate printouts as required, system logs and operational controls. As a result of audit in the first stage, if the auditor feels that the adequacy of controls requires further verifications, in the second stage he can carry out compliance testing by using the test deck method and integrated test facilities with resident audit programs. If the compliance testing exposes some control weaknesses, substantive testing may be resorted to in the third and final stage using

> retrieval software and simulation techniques with audit software. Today, many Database Management Systems (DBMS) have built-in query and report rater facilities. Unstructured queries on the data files are also possible in some advanced systems. These utilities could be profitably employed for audit purposes. The auditor will be able to obtain the relevant information from the auditee's computer centre (Basu, 2006),

The distinct advantages of retrieval packages over other methods are 100 per cent review of data and accuracy of processing and effective use of the auditor's time in analyzing results of Interrogation. Use of retrieval software will, however, always remain a problem area primarily because of the multitude of hardware and software systems in use in various departments, necessitating expertise in several programming languages.

2.8.0 Main Points to be checked in different Audit Areas

2.8.1 Audit of Acquisition

Generally the acquisition of computer facilities involves the following stages;

i.Definition of a computer policy and strategy (evaluation of organizational requirements and the ways and means of satisfying them);

ii. Establishing the need; iii. A thorough examination and evaluation of the alternative courses of action available; iv. Sþécifying precisé1ýÉVÅûirements (delineating existing and future applications, v.Hardware, software, modes of operations, conditions of supply, etc); vi. Evaluating the alternative sources of supply and selecting the most appropriate source(s), and vii. Physically acquiring the facilities and the systems

Often these stages tend to overlap or merge imperceptibly, into one another

Acquisition of computer facilities may include:

i.Acquisition of hardware involving

a. Introduction of a completely new installation

b. Enhancement of central processor,

c. Enhancement of peripherals,

d. Addition/ replacement of a specific equipment and

e. Introduction of several small computers.

f. Acquisition of software involving

g. General software associated with changes in hardware (a new operating system)

h. Specific purpose software and

i.Off her shelf application software

The auditor has to review the adequacy of administrative procedures and controls used by the auditee organization when considering and deciding upon the acquisition of computer facilities. For this purpose, he has to see that: i. a sound administrative structure exists to produce a proper analysis of the requirements of computer facilities:

ii. the acquisition procedures are effective in producing a viable computing policy and strategy

and iii. the process of evaluation and selection ensure that the requirements of the Organisation are met in the most effective and efficient way — sufficient and adequate disposal.

The auditor should direct his attention to the following areas:
i.EDP policy and strategic plan ii . Administrative structure iii. Feasibility study/ project report containing proposals, costs and benefits; equipment iv. Selection

v. Justification for hardware and software; vi. Installation of equipment and adequacy of testing and vii. Post implementation review and costs

KNUST

Feasibility study report should cover points like clear statement of objectives, existing arrangements, alternative solutions, proposed solutions, financial implications and schedule of implementation. In case of equipment selection, points to be borne in mind are;

i. Specification of requirements for acquisition, enhancement or replacement of computing facilities are stated concisely and precisely (as they form the basis for potential suppliers); ii. Both technical and commercial aspects of the proposal are evaluated according to standard contracting procedures and

Procurement action is taken after ensuring that the supplier's offers meet the requirement of the specifications by taking into account inter-alia

i.Technology options available at the time of procurement, ii. Useful life of the asset, set,

jii.—- Incidental costs which could eventually be of sufficient magnitude, besides hardware and software costs and iv. Future development plans of the potential suppliers in terms of expendability, upgradeability, etc

2.8.2 Audit of Development

Since the underlying purpose of acquisition and development (designing, building or modifying) is the same, the audit concern relating to acquisition, viz,., planning, requirements definitions, analysis of, alternatives and justification for the selected approach, are equally important in the review of systems development. Broadly stated, the audit objective of system development controls is to ascertain that procedures are adequate to ensure that the development results in well-documented computer systems incorporating adequate controls and meeting properly defined user requirements in an efficient manner. There is also a need to examine the system testing and data transfer procedures as:

i.Inadequate system testing before lien operation may result in the operation of a system which may not correctly process and record transaction and ii. Inadequate data transfer procedure may result in the relevant records being inaccurately and incompletely transferred from the old to the new system.

Where systems development is entrusted to contractors, the contract and its management become important audit concerns. It should be ensured that the vendor provides complete documentation along with source code. Further, the terms and conditions like the rights over the source code provisions for modifications/ updating in future should be examined. The penal provisions may also be examined in case of non-delivery of services/ non-adherence to time schedule. It may also be seen if any objectives could not be achieved due to_delay-in-delivery of the software (Shana Et al, 2005).

2,8.2.1 Main Points to be checked by Audit in System Development

While the auditor should be cautious enough not to be drawn into unproductive involvement in system development, the points that he should examine the following:

i.Whether a published standard methodology is being used for designing and developing systems?

ii. Whether there is a common understanding by all parties-users, systems analysts, management and auditors-of the basic structure of both manual and computer processing activities, as well as the concepts and needs for control and of the applicable control techniques? (This understanding must be reached first at a non-technical, user level) iii. Who authorizes IT applications development — the user or steering committee or management?

iv. Whether the system development work was preceded by a feasibility study to determine the most appropriate solutions to standard problems?

v. Whether there is adequate cross referencing between the following stages:

KNUST

a. Content and format of preliminary studies,

b. Feasibility studies

c. System specifications

d. Against estimates?

vi. Whether programming standards using modular structured methodology are being adhered to coding programme.

vii. Whether project management techniques are applied in system development work — that is today, there are project decision milestones, time and cost estimates so that progress could be monitored.

viii. Whether existing in house or external available application packages were considered before deciding upon new in-house application development (Shana, 2005)?

2.9 Audit of Operation and Maintenance — General Controls

Whittington Et al, 2004 discusses that the auditor has to review the internal controls, which are essential for proper operation and maintenance. The overall audit objective in reviewing the general controls is to ensure that the controls and procedures are adequate to provide secure, effective and efficient day-to-day operation of the computer facilities. The controls and procedures, which together form the general controls, are discussed in the succeeding paragraphs.

2.9.1 Organisational control

Such controls ensure that:

i. There is judicious separation of deities to reduce the risk of employee fraud or sabotage by limiting the scope of authority of any individual, ii. There are comprehensive written standards and iii. Access to and use of computer terminals is properly authorized. These high level controls are important as they influence the effectiveness of any lower level controls, which operate within accounting applications.

LIBRARY
KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY
KUMASI-GHANA

Unless management maintains appropriate IT policies and standards, it is unlikely that other controls will be sufficiently strong to support a controls reliant audit approach. An assessment of the high level IT policies, strategies and procedures will provide the auditors with reasonably reliable indications as to the existence and effectiveness of any low level detailed control

KNUST

2.9.2 Segregation of duties

The auditor should check whether adequate and effective segregation of duties has been in place amongst the staff operating the computer system as it substantially reduces the risk of error and fraud.
Poor segregation could lead to any one person, with control over a computer function, making an error or committing a fraud without detection.

Evidence of separation of duties can be gained by obtaining copies of job descriptions, organization charts and observing the activities of IT staff. Where computer systems use security profiles to enforce separation of duties, the auditor should review on-screen displays or printouts of employees' security profiles in relation to their functional responsibilities. Inadequate segregation of duties increases the risk of errors being made and remaining undetected; it also may lead to fraud and the adoption of inappropriate working practices. In any major IT System the following IT duties should be adequately segregated:

1. System design and programming ll.

System support

111. Routine IT operations and administration

IV. System security

V. Database administration

2.9.3 Physical Access and Authorization control

Physical access controls include the environment controls which operate across the whole IT environment and affect all underlying computer applications. These controls are designed to protect the computerhardware andsoftwaõffom damage, theft and unauthorized access. Access controls can operate on various levels, for example, from restricting access to the cleitn's site, to installing key locks on individual PCs. The IT Auditor should get a quick assessment of physical access controls. Restricting physical access to the IT systems reduces the risk of unauthorized persons altering the financial information.

Authorization control helps verify the identity and authority of the person desiring to attempt a procedure or an operation. This control is exercised through use of passwords, signatures, smart cards, cryptographic systems etc. such-controls ensure that only an authorized person has access to the system and its use, to enter and/or alter transactions, to take information etc.

2.9.5 Logical Access control

David C. 2006 discusses that logical Access controls are provided to protect the financial applications and underlying data files from unauthorized access, amendment or deletion. Logical access controls can exist at both an installation and application level. Controls within the general IT environment restrict access to the operating sytem, system resources and applications, whilst the application level controls restrict user activities within individual applications.

Logical access control can also be used to restrict the use of powerful systems utilities, such as file editors. Logical access controls are often used with physical access control to reduce the risk of the programs and data files being amended without authority. The importance of logical access controls is increased where physical access controls are less effective, for example, when computer systesm make use of communication networks (LANs and WANš). The existence of adequate logical access security is particularly important where a client makes use of wide area networks and global facilities such as the internet. The most common form of logical access control is login identifier (ids) followed by password authentication. For passwords be effective there must be appropriate password policies and procedures, which are known to all staff and adhered to. Menu restrictions can be effective in controlling access to applications and system utilities.

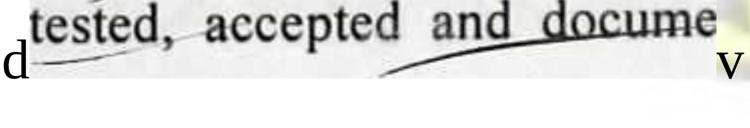
Systems may be able to control access by identifying each individual user through their unique login ids and then having a pre-defined profile of authorized menus for each. The IT Auditor should consider how each it would be for users to 'break out' of the menu system and gain unauthorized access to the operating system or other applications. Some computer systems may be able to control user access to applications and data files by using file permissions. These ensure that only those users with the appropriate access rights can read, write, delete or execute files.

2.9.6 Operation and Files Controls

Operation and file controls are meant to ensure safeguarding the computer and computer files from unauthorized access, loss or theft. Controls relating to reception, conversion and processing of data and distribution of the final output promote the completeness and reliability of these operations and safeguard against the unauthorized processing of data or programmes. File controls and procedures adequately safeguard files and software against loss, misuse, theft, damage, unauthorized disclosure and accidental or deliberate corruption. As the computer provides a means of holding, assessing and amending information, it is imperative that its use is controlled. There should be a define schedule of work that is authorized to run on it and restrictions should be placed on the number and type of staff allowed access to it. Also, computer files are records of an organization, which have to be safeguarded (David C. 2006).

2.9.7 Change Management Controls

Change management controls are used to ensure that amendments to a computer system are properly authorized, tested tested, accepted and docume v nted. Poor change controls could result in accidental or



malicious changes to the software and data. Poorly designed changes could alter financial information and remove audit trails. Audit should ensure that a new or amended computer system is thoroughly tested by its end users before live use. Financial systems rarely remain static and are frequently changed, amend or updated. These regular changes may be necessary t improve efficiency, functionality or remove programming fault ('bugs').

IT Audit should emphasize that auditee organizations which update their computer systems should have appropriate change management and configuration management controls. Configuration management procedures relate to the control of IT assets (i.e. hardware, software, documentation and communications) and the subsequent update of records, whilst change management relates to the authorization, impact assessment, asset update, testing and implementation of changes. Risks can be reduced by appropriate change management controls. These controls should ensure that all system and program amendments are satisfactorily justified, authorized, documented and tested and that an adequate audit trail of the changes is maintained. All change procedures should be documented. These controls should ensure that program and file amendments are authorized, logged and monitored. The ability to introduce new programs should be limited to authorized change control staff who are independent of computer programmers and staff who input transactions or maintain standing data.

2.9.8 Network Communication Security Controls

Network communication security controls are important where LANs/ WANs or web enabled systems are in use. Some important aspects to be covered by this control are as follows;

i. All sensitive information in the network shöuld be protected by using appropriate techniques; ii. The critical network devices such as routers, switches and modems should be protected from physical damage; iii. The network configuration and inventories should be documented and maintained; iv. Prior authorization of the Network Administrator should be obtained for making any changes to the network configuration.

v. The changes made in the network configuration should be documented. The treat and risk assessment of the network after changes in the network configuration should be reviewed.

vi.The network operation should be monitored for any security irregularity. A formal procedure should be in place of identifying and resolving security problems.

vii. Physical access to communications and network sites should be controlled and restricted.

viii. Communication and network systems should be controlled and restricted to authorized individuals.

ix. Network diagnostic tools, e.g., spectrum analyzer protocol analyzer should be used on a need basis.

x. Firewalls: Intelligent devices generally known as "firewalls" should be used to isolate an organization's data network from any external network. Firewall devices should also be used to limit network connectivity from unauthorized use.

Networks that operate at varying security levels should be isolated from each other by appropriate firewalls. The internal network of the organization should be physically and logically isolated from the Internet and any other external connection by a firewall. All firewalls should be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter. All web servers for access by Internet users should be isolated from other data and host servers.

xi. Connectivity: Organisations should establish procedures for allowing connectivity of their computer network or computer system to any outside computer system or networks. The permission to connect —her—networks o and computer system should be approved by the Network Administrator and documented. All unused connections and network segments

should be disconnected from active networks. The computer system/ personal computer or outside terminal accessing an organization's host system must adhere to the general system

KNUST

security and access control guidelines. The suitability of new hardware/ software particularly the protocol compatibility should be assessed before connecting the same to the organization's network. As far as possible, no internet access should be allowed to database server/file server or server hosting sensitive data. The level of protection for communication and network resources should be commensurate with the critically and sensitivity of the data transmitted.

xii. Network Administrator: Each organization should designate a properly trained "Network Administrator" who is responsible for operation, monitoring security and functioning of the network. The Network Administrator should investigate appropriate follow up of any unusual activity or pattern of access on the computer network promptly. The system must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g. unauthorized access, virus infection and hacking. Secure Network Management Systems should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized. Only authorized and legal software should be used on the network.

2.9.9 Business Continuity Planning

The auditor should ensure that there are adequate plans to resume processing in the event of failure of computer operations. The degree of continuity planning will depend on the size of the IT department and the dependence on computer processing. A significant and prolonged loss of IT capability in a mission criticaysystem may increase the risk of the financial statements being unavailable or materially miss-stated. Disaster recovery planning for IT facilities should be treated as one element of an_organization's overall business continuity plan. The extent of disaster recovery planning and the detailed measures required will vary considerably. Organisations with large IT departments, with mainframe computers and complex communication networks may require comprehensive, up to date recovery plans which incorporate standby facilities at alternatives sites.

Disaster recovery plans should be documented, periodically tested and updated as necessary. Untested plans may be satisfactory on paper but fail when put into practice. Testing will reveal deficiencies and allow amendments to be made. The importance of adequate documentation is increased where significant reliance is placed on a few key members of the IT department. The loss of key staff, perhaps due to the same reason the computers were disrupted, may adversely affect an organization's ability to resume operations within a reasonable timeframe. Back-up copies of systems software, financial applications and underlying data files should be taken regularly. Back-ups should be cycled through a number of generations by, for example, using daily, weekly, monthly and quarterly tapes. Back-ups should be stored, together with a copy of the disaster recovery plan and systems documentation, in an off-site fire-safe. Where microcomputers are used, in addition to mini or mainframe computers, the auditor should ensure that there are also procedures for the backing-up of financial data stored on local hard disks (Sekran, 2003).

2.9.10 Important points to be checked in general controls

The following points should be covered while reviewing these controls:

i.Obtain a list of hardware including, computer, ancillary and terminal equipment in use indicating model, performance details and check the existence of this equipment:

ii. Obtain an organizational chart which is up-to-date and see how the computer fits into the overall Organisation; iii. Obtain an up to date staff organization chart of the computer department showing the relative responsibilities and authorities and note any changes on review; iv. Obtain job specification (role definition) for senior computer staff and supervisors of the ancillary section and note any changes;

LIBRARY
KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY
XUióRS1-CHANA

v. Obtain the details of standards and norms fixed for each of the functions like data control, data preparation, system operation and verify their implementation:

a. Computer utilization per shift in terms of CPU (Central Processing Unit) and peripheral use;

b. Key depressions per shift per data entry operator and error allowance;

c. Document standards and controls-batching, balancing and sequencing,

d. run to run controls maintained by system operators;

e. Whether manuals are maintained and kept up-to-date specifying the control procedures and whether they are enforced in practice through a 'test check'.

vi. Obtain and verify, existence of the following terminal controls to protect data and system integrity:

a. Physical access controls to terminal rooms;

b. Software controls through password protection and user directories; c, Logging of terminal activities by all users vii. Obtain details of security measures, both physical and system, for check and review of the following:

a. Adequacy of protection of hardware and software against risk of fire (fire prevention steps and fire fighting arrangements):

b. Maintenance of h>e-and-system software;

c. Air conditioning and protection against possible radiations, vibrations;

d. Possible industrial action, malicious action by programmers, operators, input-output staff (discontent among computer operating staff);

e. Security awareness and training provided to all employees;

f. Emergency shut-down procedures in case of power failures;

g. Safe custody of software and data files and type library;

h. Adequacy of back-up files (offsite storage included);

i.Operator access to program files and data;

j. Procedures for reconstructing files in the event of loss or disk errors/ tape errors (contingency plans);

k. Computer equipment back-up through the use of compatible equipment at other dispersed sites;

l.Computer room should be off limits to all except systems operators, hardware engineers and

m. Insurance of the installation to cover possible risk.

2.10 Audit of Operation and Maintenance — Application Controls

Application controls are particular to an application and may have a direct impact on the processing of individual transactions. These controls are used to provide assurance (Primarily to management) that all transactions are valid authorized and recorded. Since application controls are closely related to individual transactions it is easier to see why testing the controls will provide the auditor with audit assurance as to the accuracy of a particular account balance. For example, testing the controls in a payroll applicaÐn would provide assurance as to the payroll figure in a client's accounts. Before getting on to evaluation application controls, it will be necessary for an auditor to secure a reasonable understanding of the system. For this purpose, a brief description of the application should be prepared (David C. 2006);

i.Indicating the major transactions, ii. Describing the transaction flow and main output, iii. Indicating the major files maintained and iv. Providing approximate figures for transaction volume

Application Control requirements may be divided into:

i.Documentation standards ii.

Input control iii. Processing

control iv. Output control

v. Master Data File Control vi.

Audit requirements

KNUST

2.10.1 Documentation Standards

Documentation standards ensure that adequate and up-to-date system documentation is maintained. Careful updating of documentation is also important. The auditor will find documentation helpful as an aid to understanding the system but must be careful to ensure that it is up-to-date before using it).

There should be standards in auditee organization to ensure that:

i. System documentation is sufficiently comprehensive ii.

Documentation is updated to reflect system amendments and iii. A

back-ypcopy of the documentation is held

Without good documentation, it will be difficult to assure that controls will operate on continuous basis and there will also be greater likelihood of error. Good application documentation reduces the risk of users making mistakes or exceeding their authorities. A review of comprehensive, up to data documentation should aid the auditor in gaining an understanding of how each application operates, and may help identify particular audit risks.

Documentation should include:

I. A system overview;

Il. User requirements specification;

111. Program descriptions and listings;

IV. Input/output descriptions;

V. File contents descriptions;

VI. User manuals; and

Vll. Desk instructions

2.10.2 Input Controls

KNUST

The objective of input control is to ensure that the procedures and controls reasonably guarantee that:

i. The data received for processing are genuine, complete, not previously processed, accurate and properly authorized and ii. Data are entered accurately and without duplication. Input control is extremely important as the most important source of error or fraud in computerized systems is incorrect or fraudulent input. Controls over input are vital to the integrity of the system.

The controls that the auditor should evaluate are:

i.All prime—input, including chan es to standing data, is appropriately authorized.

ii. For on-line systems, the ability to enter data from a terminal is adequately restricted and controlled.

iii. There is a method to prevent and detect duplicate processing of a source document, iv. All authorized input has been submitted or, in an on-line system transmitted and

v. There are procedures for ensuring correction and resubmission of rejected data.

The controls outlined above may be invalidated if it is possible to by-pass them by entering or altering data from outside the application. There should be automatic application integrity checks which would detect and report on any external changes to data, for example, unauthorized changes made by personnel in computer operations, on the underlying transaction database. The results of the installation review should be reviewed to ensure that the use of system amendment facilities, such as editors, is properly controlled (David C, 2006).

2.10.3 Data Transmission Controls

These controls are built in to IT Applications to ensure that data transmitted over local or wide area networks are valid, accurate and complete. Organizations using networks should ensure that there are adequate controls to reduce, to an acceptable level, the risk of data loss, unauthorized transactions being added and data corruption. Some computer systems are connected to either local or wide area networks (LANs or WANs), which allow them to receive and send data from remote locations. The more common data transmission media include telephone wires, coaxial cables, infra-red beams, optical fiber and radio waves.

Applications, which transmit information across networks, may be subject to the following risks:

I. Data may be intercepted and altered either during transmission or during storage at intermediate sites;

Il. Unauthorized data may-be—introduced into the transaction stream using the communication connections; and

111. Data may be corrupted during transmission

The integrity of transmitted data may be compromised through communication faults. The auditor should ensure that there are adequate controls in place, either within the network system, or the financial applications, to detect corrupted data. The network's communication protocol, i.e. the predetermined rules that determine the format and meaning of transmitted data, may incorporate automatic error detection and correction facilities. It is fairly easy to intercept transmitted data on most local and wide area networks. Inadequate network protection increases the risk of unauthorized data amendment, deletion and duplication. There are a number of controls that may be used to address these problems:

LIBRARY
KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY

- Digital signatures may be used to verify that the transaction contents are intact and that the transaction originated from an authorized user;
- Data encryption techniques may be used to prevent the interception and alteration of transactions.

KNUST

2.10.4 Processing Controls

Processing controls ensure complete and accurate processing of input and generated data. This objective is achieved by providing controls for:

i.Adequately validating input and generated data,

ii. Processing correct files, iii. Detecting and rejecting errors during processing and referring them back to the originators for re-processing,

iv. Proper transferof datiÞyonvprocessing stage to another, and

v. Checking control totals (established prior to processing) during or after processing.

The objectives for processing controls are to ensure that:

- Transactions processing is accurate; complete, are unique (i.e. no duplicates)
- Transactions processing is complete;
- Transactions are unique (i.e. no duplicates);
- All transactions are valid; and the computer processes are auditable.

Processing controls within a computer application should ensure that only valid data and program files are used, that processing is complete and accurate and that processed data has been written to the correct files. Assurance that processing has been accurate and complete may be gained from performing a reconciliation of totals derived from input transactions to changes in data files maintained by the process. The auditor should ensure that there are controls to detect the incomplete or inaccurate processing of input data. Application processes may perform further validation of transactions by checking data for duplication and consistency with other information held by other parts of the system. The process should check the integrity of data, which it maintains, for example, by using check sums derived from the data. The aim of such controls is to detect external amendments to data due to system failure or use of system amendment facilities such as editors.

Computerized financial systems should maintain a log of the transactions processed. The transaction log, which may be referred to as the audit trail file should contain sufficient information to identify the source of each transaction. In batch processing environments, errors detected during processing should be brought to the attention of users. Reject batches should be logged and referred back to the originator. should incorporate controls to monitor and report on unprocessed or

unclean transactions (such as part paid invoices). There should be procedures, which allow identifying and-reviewing all un-cleared transactions beyond a certain age (David C. 2006).

2.10.5 Master/ Standing Data File Controls

Master/ Standing Data File controls are meant for integrity and accuracy of Master Files and Standing Data. Accuracy of data on Master and Standing files is of vital importance, to the auditor. Information stored in master and standing data files is usually critical to the processing and reporting of financial data. Information on master files can affect many related financial transactions and so must be adequately protected. These have to ensure that:

i. Amendments to standing data are properly authorized and controlled.

ii. Integrity of Master and Standing Files is verified by checking, control totals and periodic reconciliation with independently held records.

iii. Special amended facilities are properly recorded in and then use controlled by management authorization and subsequent review and physical and logical access to application data files are restricted and controlled.

2.10.6 Audit Requirements

Audit requirement have to be provided to ensure that the system can be audited in an effective and efficient manner. Audit trail has to be maintained to enable tracing of an item from input through to its final destination and break up a result into its constituent parts. (Auditors may have to use audit software or test data for the efficient execution of their audit. They have, therefore, to seek reasonable request for the access to copies of system data files, report generators and processing time). Before considering the audit requirements for a system being developed, the auditor should have a knowledge ofthè currently existing system and should keep in mind:

i. Weakness in the current system affecting the audit approach,

LIBRARY
KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY

ii. Features in the existing system, which are relied on to provide an effective audit, that should be retained in the new system, and iii. Additional facilities, not currently provided which would assist the audit of the new system.

2.11 Audit Trail

Objective of audit trail is to obtain sufficient evidence matter regarding the reliability and integrity of the application system. To achieve this, trail should contain enough information to allow management, the auditor and the user:

i. To recreate processing action to verify summary totals and to trace the sources of intentional and unintentional errors.

The audit trail should include the following information:

- System information, which includes start up time, stop time, restarts, recovery etc
- Transaction information including input items which change the database, control totals and rejected items relevant to database applications).

- Communication information including terminal log-on/off, password use, security violation, network changes and transmission statistics (relevant to transaction processing i.e. TP applications)

KNUST

CHAPTER 3

METHODOLOGY

3.0 Introduction

This chapter of the study discusses the study area, research design, population sampling, procedure, sample size, and research instruments and data analysis.

3.1 Study Area

3.1.1 Union Savings and Loans Company Ltd.

Union Savings and Loans Company Ltd has six branches in Ghana, there are three branches located in the Kumasi metropolis, two branches in Accra and one branch in Takoradi. The head office is located in Accra, the nation's capital and house the top management of the institution. It is headed by a Managing Director and has five departments each having its head namely Credit Risk Department, Finance and Administration, Customer service Department, Internal control and the Business Division Department. Most decision are made by the Management which consist of the Managing Director and his five department heads, there is also the Board of Directors which consist of the Managing Director , the Board chairman and four non Executive members who also make decisions which do affect the Company.

For purposes of effective performance of its functions, the Company has decentralized its functional and administrative machinery-by-establishing Branch managers and other functional managers in each Of the Branches who report directly to the Departmental Heads in Accra. Each of the Branches is headed by the Branch manager and they are responsible for every business and decisions that takes place in the Branches.

The Company recognizes the importance of staff development and has designed elaborate programmes of action with a focus recruitment, training, discipline and retention. Its programme on-the-job training and staff promotion has been continuous and impressive. It regularly sponsors senior and junior staff to upgrade their knowledge at regular trainings and workshops.

KNUST

3.2 Research Design

A research design is a framework for conducting a research. It details the procedures necessary for obtaining information needed to solve a research problem (Malhorta and Birks, 2007). The survey method was adopted for this study. This is because the method allowed one to collect quantitative data which can be analyzed using descriptive and inferential statistics (Saunders, Lewis and Thornville, 2007).

3.3 Research Population

The target population for this study consisted of all the staff of Union Savings and Loans Company Ltd and the staff of Charles Allotey & Co. This includes the 10 internal Auditors, five IT staff and ten regular staff of Union Savings and Loans Company and fifteen staffs of their external Auditors, Charles Allotey & Co.

3.4 Sampling Frame

The sample frame for this study focused on all the staff of Union Savings and Loans Company Ltd which includes-their Auditing-stãTTš-W4óaffs and the regular staff of the company. The sample unit in Charles Allottey & Co also consists of their employees in the Kumasi Metropolis.

3.5 Sampling Procedure

In considering the population size, which is relatively small in number, almost all the staff who are internal auditors and IT staff were selected. The external auditors of Charles Allottey and co were selected base on a systematic random sampling. The other regular staffs of USL, who are ten in numbers, were selected base on a systematic random sampling.

3.6 Sampling Size

The study relied on the published tables which provide a sample size for a given set of population. The sample size selected for this study was generated from the sample size determination tables. The Sample size for this study by the table was 40 with a 95% level of confidence of 0.05 margin of error.

Figure 3.1 summaries the sample section for the study

Figure 3.1 Sampling size determination

Categories of Respondents	Sampling size	Sampling technique	Instrument
Interval/External Auditors with IT	20	Census	Questionnaire
IT Technician	5	Purposive	Interview
Staff	10	Purposive	Interview
Non IT Auditors	5	Purposive	Questionnaire
TotaY	40		

3.7 Sources of Data

Both primary and secondary data were gathered for the study. According to Malhotra and Birks (2007), the researcher should locate and analyze secondary data before collecting primary data. They indicated that secondary data which are data that have already been collected for purposes other than the problem at hand can help in sample designs and in the details of primary research methods. For this reason, the researcher first reviewed existing literature from textbooks and the internet. Realizing that the secondary data could not give sufficient data for the study, the researcher used primary data as well. Primary data are data originated by the researcher specifically to address the research question at hand. The primary data for the study was generated using questionnaires and interviews.

3.8 Data Collection Instruments

Designing a good questionnaire always takes several drafts. The first draft concentrated on the content. The second took critical look at the formulation and sequencing of the questions. Then the formats of the questionnaire were scrutinized. Finally, a pilot test was conducted to check whether the questionnaire yielded the data required and whether interviewers as well as respondents felt at ease with it. The questionnaires finally used consisted of completely open-ended as well as closed-ended questions.

KNUST

3.9 Data Collection Procedure

The questionnaires were personally given out to the respondents. The researcher personally collected all completed questionnaires from the respondents at the point where the questionnaires were administered to them. Instances where the respondents were not able to fill the questionnaire at the first time of administering it, another day was rescheduled for the collection. The researcher scanned through each questionnaire after it had been filled out to ensure that the respondents answered all

NYANSAPƆ WƆSANE NO BADWENMA

relevant questions. The researcher, however, respected ridg of any respondcrg who did •ns•cr some of the questions or the questionnaire as a whole.

3.10 Data Presentation and Analysis of Results

The data analysis consisted of examining the surveys for correctness and completeness, coding and keying data into a database in Statistical Package for Social Sciences version (SPSS). arui performtng an analysis of descriptive responses. All incomplete responses were discarded from analysis. Frequency tables, Graphs, Pie charts and descriptive statistics were constructed to display results with respect to each of the research questions.

3.11 Ethical Considerations

According to Sekran (2003) ethical issues should be addressed while collecting data. This may include the purpose of the research, confidentiality of data obtained, respect of the participant in all aspects. and not forcing the participants in case he/she takes time to respond. Emory (1985) pointed the various unethical issues in research, which need to be avoided include violating nondiElosure agreements, breaking respondent confidentiality, misrepresenting results and deceiving people.

During the study strict compliance was ensured with regard to the guidelines by Homan. (1991) for the need to explain the purpose of study and the benefits expected from respondents. the rights of respondents and how these would be protected and kept confidential and obtaining thc infortrxd consent of respondents duringibe-processof interviews. In this study therefore. it was ensured tha the fundamental aspects of ethical consideration were complied wiOL Participargs wcrc ass•ged of full confidentiality of their identity (personal) and the information provided.

CHAPTER FOUR

PRESENTATION AND DISCUSSION OF FINDINGS

4.1 Introduction

This chapter presents the analysis of data collected as well as the discussions of the findings. The analysis covers the effects of IT in Audit practice, the extent IT facilitates the detection and minimization of fraud in Union Savings and Loans, the reaction of Auditors to the introduction of new technology and the Challenges to the use of IT in the financial Industry.

4.2 Effects of IT in Audit Procedure

When the respondents were asked whether the use of IT in audit procedure affects it operations positively, majority of the respondents is 87.5% answered in the affirmative. They explained that the use of IT impacts positively on the operations of Auditors by facilitating the operations of Auditors through providing fast records of transactions and information when retrieving. 12.5% of the respondents however stated that the use of IT in Audit procedures has no impact at all; their explanation was that as a result of the use of obsolete PCs, slow network connectivity inefficient banking and software frequent machine breakdown: This implies that IT help the performance of Auditors in their work at the company, the company must do well to replace the obsolete PCs, install more efficient Banking softwares and improve upon their network connectivity.

LIBRXRY

Effects of IT	Frequency	Percentage
Positive Impact	35	87.5
No Impact	5	12.5

KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY
KUMASI-GHANA

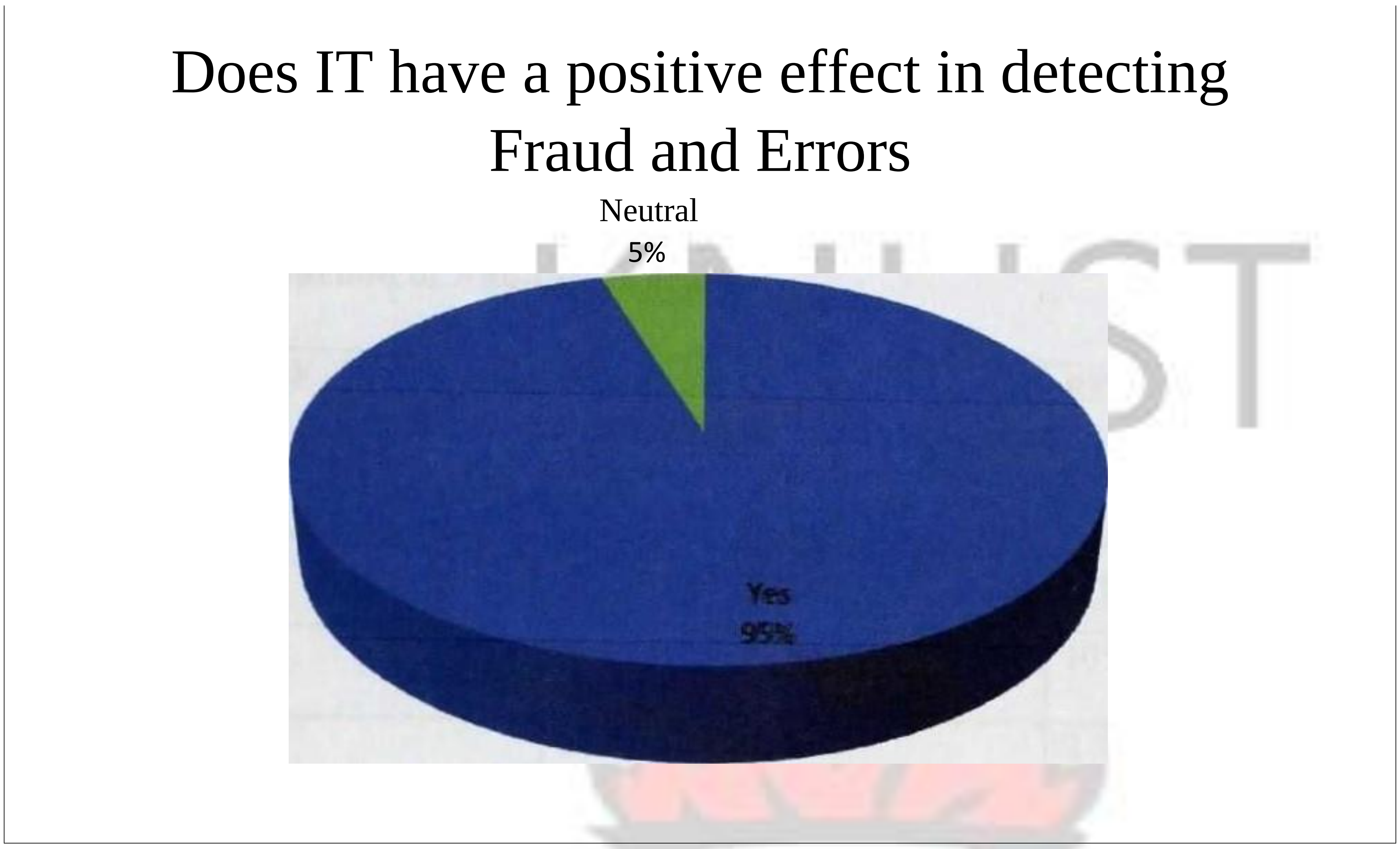
Total	40	100.00

Source: Field Data, 2013

4.3 How IT has affected the Detection of Fraud and Error

The detection of fraud and error is aided by the effective and efficient use of technology. Auditors claim they always have to learn new ways to use technology to fight fraud with each project that they undertake since criminals continue to use advance IT knowledge and learn new ways and different technique in perpetrating fraud. However, the implementation of IT controls has helped to minimize it. So there is the need for Auditors to be very conversant to new technology trends so as not to be outsmarted by these criminals. This is evidenced by the pie below

Figure 4.3.1 IT and Fraud detection.



Source: Field Data, 2013

From figure 4.3.1 , when respondents were asked whether the use of IT has help in Auditors detection of Fraud and Errors, 95% ofthe respondent were ofthe view that IT has help the detection of fraud and errors, none of the respondents think otherwise and only 5% were not sure the effect of IT in

Auditing for detecting Fraud and Errors.

4.4 Auditors' Reaction to New Technology

It is determined that-there are three categories of people who live in this computer age. The first categories are those who adopted IT very early, understood its emergence, and looked for ways to makeit Work in their worlds. The second category however is against change. Most auditors identify themselves and their companies as pragmatics- The third category is the technological laggards who have not advanced as quickly as other companies.

According to an audit manager in a large organization, 'It is not an auditor's job to tell the organization what technology to use'. He feels that he must link his efforts with those in the information services group who choose and deploy new technologies.

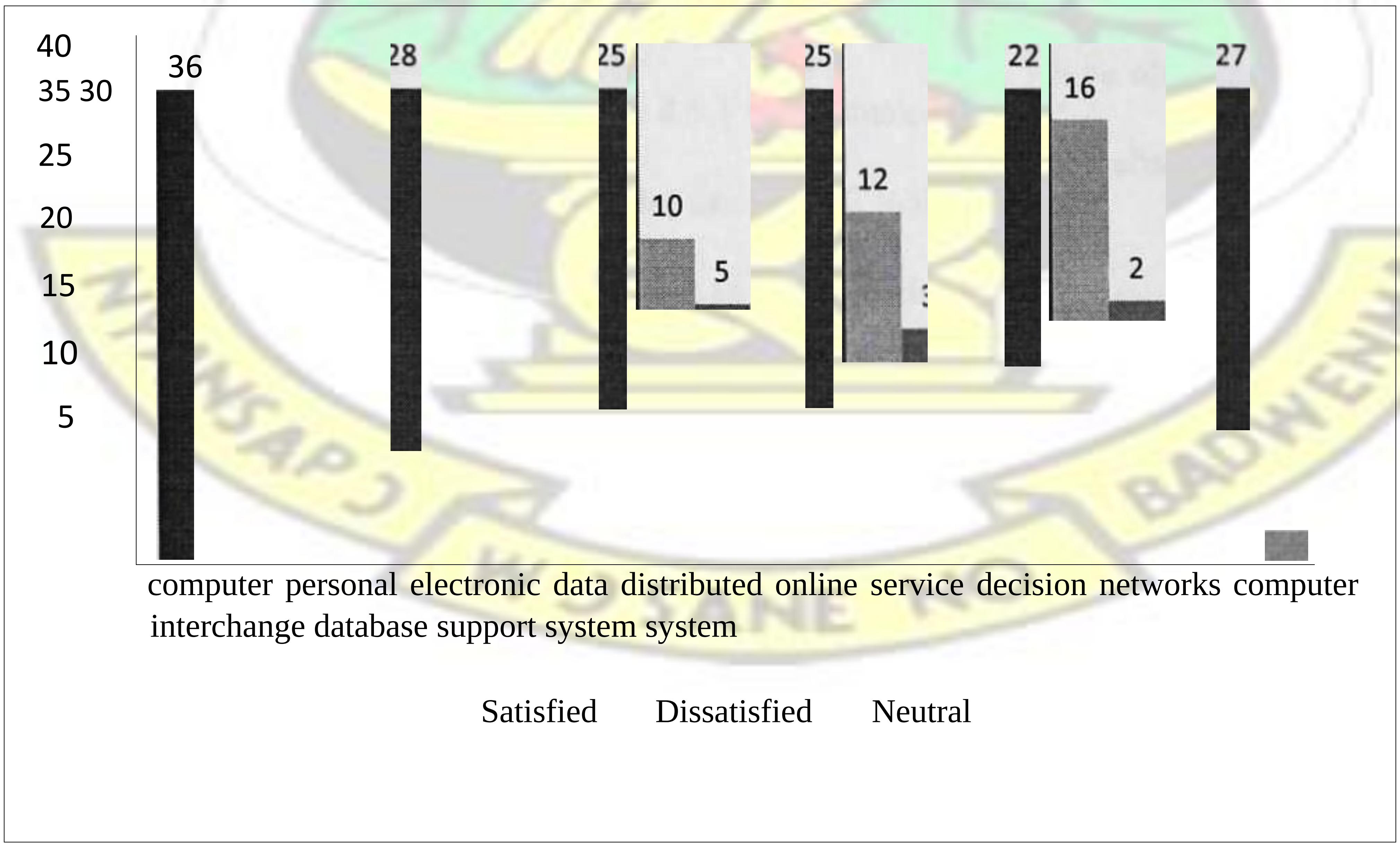
Figure 4.4.1 Reaction of Auditors to change

REACTION OF PERSONNEL	NUMBER	PERCENTAGE
WELCOMED	35	87.5%
RESISTED	4	
NEUTRAL	1	2.5
TOTAL	40	100

Source: Field Data, 2013

From Figure 4.4.1 it can be concluded that most Auditors have seen the significance of IT use in their operation and therefore have welcomed IT introduction. Those who have either resisted or remained neutral to it are those who lack knowledge on IT use. From the Graph 4.4.2 it is realized that most auditors are satisfied.

Figure 4.4.2: Satisfaction of Auditors



Source: Field Data, 2013

The graph gives diverse opinion and it can be deduced that many of the survey respondents are dissatisfied with their ability to audit new technology better.

Auditing was surveyed specifically about their satisfaction with auditing methodology for various information technologies. Over 40% and 70% of survey respondents were dissatisfied and satisfied respectively with their methodologies to audit the various new technologies. While information technologies do present a challenge, the degree of dissatisfaction is worrisome. Graph 4.4.2 shows the degree of dissafisfaction or only moderate satisfaction for organizations.

Auditors who have not been trained are more often dissatisfied with auditing methods for new technologies. Auditors who are trained in the use of IT are less dissatisfied, perhaps indicating an overall healthy attitude in an industry where training is considered important.

Dissatisfaction with auditing methods varies with the technology being discussed. Topping the list of risky technologies is on-line services, which include the Internet where most concerns are expressed.

4.5 Challenges to the Effective Implementation of ICT in Union Savings and Loans Ltd

In response to the question on the challenges the respondents faced in the use of ICT tools at Union Savings and loans, the results in Table 4.5.1 were obtained. It can be observed that the most common challenges the respondents faced in the use of ICT tools were the absence of internet connectivity, frequent power outages and the delays due to personalizing.

Figure 4.5.1: Challenges faced by respondents in the use of ICT tools

Challenges	Frequency	Percentage (0/0)
Absence of internet connectivity	12	30.00
Virus attack	8	20.00
Unavailability of the technological know how	3	7.50
Frequent power outages	4	10.00

KNUST

Delays due to personalizing of PCs	2	5.00
Tools are obsolete	8	20.00
Electrical failure	1	2.50
Lack of maintenance	2	5.00
Total	40	100.00

Source: Field Data, 2013

4.8 Auditors' Use of Technology

All things being equal, Internal Auditors use a wide variety of technology during the course of the Audit. However, the study shows that the heaviest use of technology is focused on workflow related tools such as computer networks, e-mails, electronic working papers and presentation graphics. By comparism, technologies that directly support the auditing process such as file interrogation, automated risk analysis, decision support and neutral networks, are also used.

4.9 Union savings and loans limited

Savings and loan companies are being regulated by Bank of Ghana regulations. Their affairs are being audited by Bank of Ghana yearly to determine and make sure that their activities conform to lay down rules.

As part of policies on setting up a savings and loans company they have to be Audited-occasionally. As part of having an effective control system two types of auditors are used in the savings and loans sectors. They are the internal control department and external auditors.

The internal control department forms part of the administrative hierarchy of savings and loans companies and includes the head and his internal Auditors. They go round the different branches of the organisation to make sure that work is done according to the rules and policies of the institutions. Sometime and queries are issued out to worker who goes contrary to these rules and regulations.

All savings and loans companies are required by law to have external auditors. These auditors are responsible in preparing their financial statements and also having independent impressions in the operations in the savings and loans. Their reports always go straight to the Board of the Company for an effective decision to be made.

Union savings and loans limited have been incorporating IT in their operative since 2000. The company started out operations in 1997. Its operations were mainly manual. The following shows how the implementation process has gone so far down the years.

KNUST

1. In 2000 computers were introduced in their operative and with the introduction of computer comes a new banking software called
2. In 2009 due to the shortfalls of the Banking software the smart bank software was introduced. This software was quite advance as compared to the previous one and propelled the company into an IT oriented company. The smart bank has features that supports Auditors and have effective control system in place. Some of its features is the Audit trail.
3. In 2012 however the smart bank became obsolete as it was not able to keep up with new financial trends which make reporting easier, The institution embarks on a massive IT implementation so as to catch competition in their industry and also to have an effective control mechanism in place. The status was introduced to replace the smart bank. The status is more Auditor friendly as compared to the smart bank and helps control the affairs of the institution. All the branches were all networked. This makes it easier for the internal control department to monitor the companies operations.
4. Large deliveries at IT infrastructure were put in place like laptops, servers, printers Desktops to support the new platform. These have made union savings and loans having their operatives solely-in based. An-AadfiöñQill have to be at least in IT and it is application wonder to perform his duties in the company. I must also say that even though most of their work are perform on their IT platforms a good number are still manual. There is always a daily effort by the management of the company to upgrade their IT infrastructure so as not to be left behind in an ever-changing industry.

KNUST

CHAPTER FIVE

SUMMARY, CONCLUSIONS & RECOMMENDATIONS

5.1 Introduction

This chapter summaries the findings, conclusions on the findings and provides recommendations on the research conducted. The main focus of this research was on the impact of IT on Audit practice:
The case ofUnion Savings & Loan Company Limited.

5.2 Summary

The study specifically examined how IT has affected Audit procedures and findings, how IT has facilitated the detection and minimization of the occurrence of fraud and error, the software used in organizations and IT auditing and the problems associated with the use of IT on its procedures. The population included the internal and external auditors of union savings loans and their staff. A sample size of 40 was chosen for the study. The instrument used for the collection of data was questionnaires, which consisted of both closed and opened-ended questions. The data collected were analyzed through the tabular and graphical representation.

5.3 Summary of main findings

Based on the findings it has been realized that the main problems faced in the implementation of IT are non-availability of funds and lack of knowledge of Audit personnel on IT use. Most of organizations find it difficult in implementing IT due to lack of funds for setting up IT equipment and tra-iñi-ng Audit personnel. Auditors who are dissatisfied with the use of IT in Audit methodology are those who lack knowledge on its usage and therefore neutral to the new change in Auditing, their possibilities of making mistakes is high.

LIBRARY
KWAME NKRUMAH UNIVERSITY OF
SCIENCE AND TECHNOLOGY

SUMAS] -GHANA

Although the organizations face certain problems in implementing IT, they also generate many benefits from its use.

a) Firstly, Auditors claim that the possibilities of making mistakes during Auditing have decreased drastically.

b) Secondly, the rate and manner in which Auditors carry out Audit procedures has improved economically, effectively and efficiently. This is in comparism to the ordinary method of Auditing where a number of stationery items were needed, Auditors had to travel long distances several times, accumulate several receipts and vouchers for casting and vouching among others.

c) Thirdly, it has been identified that IT has facilitated the detection and minimization of the occurrence of fraud and error due to the improved implementation and use of IT controls.

The study further revealed that there are different forms of IT systems such as personal computers, computer networks; electronic data interchange, distributing processing systems, on-line service and decision support system.

5.4 Conclusion

From the results of the study, it is quite clear that IT has made a positive impact on the practice of an Audit. With regard to this, Auditors are eager to learn the new ways IT has provided in carrying out an Audit. Organizations are alsg_jns.ta4kngÆT equipment and training employees on the use of IT.

Society in general has accepted the introduction of IT in business operations and specifically Auditing. However, some Auditors who lack knowledge on its use has either resisted or remained neutral on its introduction even though they confessed they have realized a great difference in the improvement of the output of their colleagues (IT Auditors).

It can therefore be concluded from the results of this study that Auditors and organisations have realized the effective, efficient and economic use of IT on Audit practice and the need to upgrade their knowledge to enable them meet the demands of their changing roles and the environment.

5.5 Recommendations

The findings of the study and the conclusions drawn provide a number of recommendations

a) Organizations should include in their budget an amount to install IT equipment and/or to train Auditors on it use.

b) Organizations should implement an efficient Audit trail to secure data transactions and hence facilitate the detection and minimization of the occurrence of fraud and errors.

c) Government should minimize the import duties on IT equipment to enable companies to afford the cost of purchasing and installing them in their offices.

d) Government should organize regular workshops to educate and train employees of organizations, especially savings & loans companies on the importance of IT use and IT Audit to its operations. This will motivate Management of organizations to further train employees and implement IT infrastructure.

REFERENCES

A.H.Millclamp — (2005) Auditing.

C.A Stranivasan Anand, (2011) Students Guide to Advanced Auditing & Professional ethics.

David C. (2006) Evolution of information systems: Principle of Auditing and management information systems. http://www.hkiaat.org/images/uploads/articles/AATpaper80ct09.pdf

David E. Nye —(2007) Technology Matters: Questions to line with S. K Bonsu 2006 Auditing: Principles and Techniques.

Emery C. W. Homewood IL: Richard D. Irwin, (1985), Research Methods

Homan, R. (1991) The ethics of Social research London. : Longman House. National Health and Medical Research council (2003a). Human research ethics handbook Retrieved Date:28/05/13 .

KNUST

KNUST

Http//www.nhmrc.gov.au/publications/synopses/e42syn.htm.

International Organisation of Supreme Audit Institutions. Auditing Standards and guidelines ISSAI, 3000 .

James P. Russel (2005) — The Quality Audit Handbook Principles, Implementation and use.

Jekran Y. (2003), Research Methods for Business. A skill Building approach 4th edn. (New York: Willey).

Jimenez- Zarco, (2006) Analysis of ICTs opportunity on firms success: An innovation process, problèms and perspective in management.

K. H. Spencer Pickett (2004) — The Internal Auditor at work a practical Guide to Everyday challenges.

Mary Ellen Fisher (1996), Electronic Commerce: Profiting from business online.

Naresh K. Malhotra David F. Birks (2007) Marketing Research: An applied Approach.

Naresh Vaid(2003) Auditing Questions and Answers.

Nick A Dauber, Marc H. Levine, Anigne Ahmed Qureshi, Joel G. Siegel (2009) — The Complete Guide to Auditing Standards and other professional standards for Accountants.

Ray Whittington, Kurt Pany (2004) — Principles of Auditing and other assurance services.

Ravinder Kumar and Virender Shama (2005) Auditing: Principles and Practice.

Rabinora Jaggernauth, Effective use of information and Communiations. (http://www.dflcaribbean.com/investment-conference/l)jiagganauth.pdf

Rick Stephan Hayes, Roger Dassen, Arnold Schilder, Phillip Walluge — (2005), Principles of Auditing: An Introduction to International Standards on Auditing.

Spanos Y. Et al (2001), The relationship between information and communication technologies adoption and management. Information and management.

Saunders, Lewis and Thornville (2007): Research Methods for Business Student (5th edition) New Jersey.

S.K Basu (2006), Auditing: Principles and Techniques.

Tommie W. Singleton, Aaron J Singleton (2010), Fraud Auditing and forensic Accounting.

KNUST

Appendix

Kwame Nkrumah University of Science and Technology, Kumasi.

Institute Of Distance Learning

QUESTIONNAIRE

Dear Respondents,

I am a Commonwealth Executive Master in Business Administration (CEMBA) student of the Kwame Nkrumah University of Science and Technology (KNUST), Kumasi undertaking a study on "The Impact of Information Technology in Audit Practice" as a partial fulfillment of the requirements for the award of a Master Degree in Commonwealth Executive Master in Business Administration (CEMBA). I would be grateful if you could assist me achieve this aim by answering this questionnaire. You are assured of high confidentially.

Thank you

____

Jesse Kyei Peprah

1. Personal particulars

   Surname ....

   Other names ....
   . . . .

   Date of birth/age

2. Employment history

a. Organisation position held period

....

KNUST

b. Type(s) of IT at your disposal

LIBRARY
AME NKRUMAH UNIVERSITY OF

c. Type of IT instrument used in the operation ofthe business

d. The type of software used in the operation of the business

e. The type(s) of software, which are scarcely used

f. Reaction of audit personnel to change

Welcomed . ________ resisted __________ Neutral ....

g. The problem (s) and/ or difficulties faced in using them

h. How do these affect the work? . . . .

i. Duration of work . . . .

j. Possibilities of making mistakes ....

Very often ( )

Often ( )

Fairly often (

Hardly

k. How has IT affect thenanner I which Audit is conducted?

Very effective (

Effective

Less effective

KNUST

l.How has IT helped the organization of an Audit?

Very costly (

Costly

Economical

3. How is the effects of IT in Audit Procedure

Positive Impact (No

Impact

Negative Impact (

4. Do you Think IT has a positive effect on the detection of fraud and Error

Yes

No

5. What is your reaction to Technology

Welcomed

Resisted

Neutral

6. Are you satisfied with the follow' g IT tools

Satisfied Dissatisfied Neutral

a. Computer Network ( )

b. Personal Computer ( )

c. Electronic interchange ( )

d. Distributed database sys ( )(

e. Online service

f. Decision support system () (

7. What are the challenges you face in using IT in your work

a. Absence of internet connectivity ( )

b. Virus Attack

c. Unavailability of technology know how ( )

d. Frequent power outages

e. Delays due to personalizing of PCs (

f. Tools are obsolete

g. Electric failure

h. Lack of maintenance

KNUST
NYANSAPƆ WƆSANE NO BADWENMA