ST. MARY'S UNIVERSITY

DEPARTMENT OF ACCOUNTING AND FINANCE

ASSESSING PRACTICE OF INFORMATION TECHNOLOGY AUDIT AND FRAUD DETECTION ON COMMERCIAL BANKS IN ETHIOPIA

BY:
TIGIST ALEMAYEHU GISSILA

MARCH, 2021
ADDIS ABABA, ETHIOPIA

ASSESSING PRACTICE OF INFORMATION TECHNOLOGY AUDIT AND FRAUD DETECTION ON COMMERCIAL BANKS IN ETHIOPIA

A RESEARCH PAPER SUBMITTED TO St. MARY'S SCHOOL OF GRADUATE STUDIES FOR PARTIAL FULFILLMENT OF MSC. IN ACCOUNTING AND FINANCE

BY:
TIGIST ALEMAYEHU GISSILA

ADVISOR:
MOHAMMED SEID (ASS. PROFESSOR)

ST. MARY'S UNIVERSITY
SCHOOL OF GRADUATE STUDIES
GRADUATE PROGRAM IN ACCOUNTING AND FINANCE

MARCH, 2021
ADDIS ABABA, ETHIOPIA

DECLARATION STATEMENT

I declare that, this thesis is my original work and has not been present for any degree and that all sources of materials used for the study have been accordingly acknowledge.

Name: Tigist Alemayehu

Signature: ___________________________

Date: December, 2020

This thesis has been submitted for examination with my approval as a university thesis advisor of Accounting and Finance program.

Name: **Mohammed Seid (Ass. Professor)**

Signature: _________

Date: December, 2020

ST. MARY'S UNIVERSITY
SCHOOL OF GRADUATE STUDIES

ASSESSING PRACTICE OF INFORMATION TECHNOLOGY AUDIT AND FRAUD DETECTION ON COMMERCIAL BANKS IN ETHIOPIA

BY:
TIGIST ALEMAYEHU

APPROVED BY BOARD OF EXAMINERS

Dean, Graduate Studies **Signature**

_________________________ _________________________

Advisor **Signature**

Mohammed Seid (Ass. Professor)

_________________________ _________________________

Internal Examiner **Signature**

Zenegnaw Abiy (PhD)

_________________________ _________________________

External Examiner **Signature**
Dakito Alemu (PhD)

_________________________ _________________________

ACKNOWLEDGMENTS

First and for most, my deepest and warmest thanks go to the Almighty God and His Mother Saint Marry, who help me in all aspects of my life including the achievement of this thesis.

I would like to express my heartfelt gratitude to my advisor, Mohammed Seid (Ass. Professor) for the comments and supports to make this research paper and for the information given that is valuable for my study.

I am extremely thankful to my mother W/ro Alem Beyene, who passed away last week, she had great role in my life and numerous sacrifices for me.

I’d like to express my deepest gratitude to my husband, Tewodros Yazew, and my Sister Tidenek Alemayehu for their patience and tolerance over the last two years. Thank you for being with me and for your appreciated sacrifices. Thank you my quite children, Nathan, Amen, and Bethlehem, for being good kids with your mother when I was studying in the School.

I am also very thankful to ECX Internal Audit Department Staffs, especially Ato Teferi Lemma, Jemal Nasir and Yordanos Yalew and my friends Hirut Letike and Menbere Tsegaye and Tadelech Lashitew who were always so helpful and provided me with their assistance during my thesis.

Table of Contents

DECLARATION STATEMENT i

ACKNOWLEDGMENTS iii

LIST OF TABLES viii

ABBREVIATIONS/ACRONYMS x

ABSTRACT xi

CHAPTER ONE 1

1. INTRODUCTION 1

1.1 STATEMENT OF THE PROBLEM 2

1.2 RESEARCH QUESTION 4

1.3 OBJECTIVE OF THE STUDY 4

1.3.1 GENERAL OBJECTIVE 4

1.3.2 SPECIFIC OBJECTIVE 4

1.4 SIGNIFICANCE OF THE STUDY 4

1.5 SCOPE OF THE STUDY 5

1.6 LIMITATION OF THE STUDY 5

1.7 STRUCTURE OF THE THESIS 5

CHAPTER TWO 6

2 LITERATURE AND EMPIRICAL REVIEW 6

2.1 THEORETICAL LITERATURE 6

2.1.1 DEFINITION OF IT AUDIT 7

2.1.2 THE NEED FOR IT AUDITING 8

2.1.3 IT AUDIT OBJECTIVES 9

2.1.4 IT CONTROLS 10

2.1.5 AREAS COVERED THROUGH IT AUDIT 11

2.1.5.1 IT GOVERNANCE 11

2.1.5.2 PHYSICAL ACCESS CONTROL 12

2.1.5.3 LOGICAL ACCESS CONTROL 12
2.1.5.4 IT ASSET MANAGEMENT 12
2.1.5.5 DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN 13
2.1.5.6 DATA BACK UP AND RESTORATION 13
2.1.5.7 DATA PROTECTION AND PRIVACY 13
2.1.5.8 IT APPLICATION CONTROL 13
2.1.5.9 NETWORK SECURITY 14
2.1.6 CHALLENGES FACED IN CONDUCTING IT AUDIT 14
2.1.7 DEFINITION OF FRAUDS 15
2.1.8 IT RELATED FRAUD 16
2.1.9 IT AUDIT DETECTION APPROACHES AGAINST IT RELATED FRAUDS 19
2.2 EMPIRICAL LITERATURE 21
CHAPTER THREE 24
3. RESEARCH METHODOLOGY 24
3.1 RESEARCH DESIGN 24
3.2 RESEARCH APPROACH 24
3.3 RESEARCH POPULATION 24
3.4 SAMPLE SIZE 25
3.5 DATA COLLECTION 25
3.6 DATA ANALYSIS AND INTERPRETATION 26
3.7 VALIDITY OF THE STUDY 26
3.8 RELIABILITY 27
3.9 ETHICAL CONSIDERATION 28
CHAPTER FOUR 29
4. DATA PRESENTATION ANALYSIS AND DISCUSSION OF RESULTS 29
4.1 RATE OF RESPONSE 29

4.2 DEMOGRAPHIC CHARACTERISTICS OF RESPONDENTS..29

4.3 IT AUDIT PRACTICE AND FRAUD DETECTING APPROACHES...............................33

4.3.1 IT AUDIT FOCUSED AREA 35

4.3.1.1 LOGICAL AND PHYSICAL CONTROL AUDIT 35

4.3.1.2 IT ASSET MANAGEMENT AUDIT 36

4.3.1.3 DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN AUDIT 37

4.3.1.4 DATA BACKUP AND RESTORATION AUDIT 37

4.3.1.5 DATA PROTECTION AND PRIVACY AUDIT..38

4.3.1.6 DATACENTER MANAGEMENT AUDIT 39

4.3.1.7 SYSTEM AVAILABILITY AUDIT..39

4.3.2 CHALLENGES FACED IN CONDUCTING IT AUDT...40

4.3.2.1 LACK OF AUDIT RESOURCES (TOOLS) USES DURING IT AUDIT............40

4.3.2.2 CHALLENGES OF COPING WITH TECHNOLOGY CHANGES 41

4.3.2.3 POOR ASSESSMENT OF THREAT AND VULNERABILITY 41

4.3.2.4 DIFFICULTIES ON THE IDENTIFICATION OF IT RISKS 42

4.3.2.5 LACK OF MANAGEMENT APPRECIATION 42

4.3.2.6 LACK OF AUDITORS IT CONTROL KNOWLEDGE.......................................43

4.3.3 IT RELATED FRAUDS...44

4.3.3.1 UNAUTHORIZED NETWORK ACCESS...44

4.3.3.2 SNIFFING 44

4.3.3.3 HACKING...45

4.3.3.4 DATA INTERCEPTION DURING FILE UPLOAD 46

4.3.3.5 INSIDER THREAT...46

4.3.3.6 PHISHING...47

4.3.3.7 MALWARE PROGRAMS..48

4.3.4 IT AUDIT AND FRAUD DETECTION APPROACHES...49

4.3.4.1 NETWORK SECURITY ANALYSIS 49

4.3.4.2 PORT SCANNING 49

4.3.4.3 VULNERABILITY SCANNING 50

4.3.4.4 PHYSICAL SECURITY CHECKS ON IT ASSETS 50

4.3.4.5 USES OF DATA ANALYSIS 51

CHAPTER FIVE 52

5. SUMMARY, CONCLUSIONS AND RECOMMENDATION 52

5.1 SUMMARY OF THE STUDY 52

5.2 CONCLUSION 53

5.3 RECOMMENDATION 54

5.4 SUGGESTIONS FOR FURTHER STUDY 54

REFERENCES 55

APPENDIX 60

LIST OF TABLES

Table 1:-Name of commercial banks in Ethiopia based on ownership 25

Table 2:-Reliability of statistics 27

Table 3:- Distribution of Respondents by Age 30

Table 4:- Distribution of respondents by work experience 31

Table 5:- distribution of respondents by IT audit experience 32

Table 6:- Distribution of respondents by professional certification 32

Table 7:- who conduct IT audit 33

Table 8 :- how often conducting IT audit 33

Table 9:- IT audit reference guideline 34

Table 10 :- types of IT audit report 34

Table 11:- reporting structure of IT Auditors 35

Table 12 :- Practice of logical and physical control audit 36

Table 13:- Practice of IT asset management audit 36

Table 14:- Practice of Disaster recovery and business continuity plan audit 37

Table 15:- Practice of Data backup and restoration audit 38

Table 16:- Practice of data protection and privacy audit 38

Table 17 :-Practice of datacenter management audit 39

Table 18 :- Practice of system availability audit 40

Table 19: Lack of IT audit tools 40

Table 20:-Challenges in coping technology changes 41

Table 21:- Poor assessment of threats and vulnerabilities 42

Table 22:- Difficulties on the identification of IT risks 42

Table 23:- Lack of management appreciation on the importance of IT audit 43

Table 24:- IT control knowledge gap by IT auditor 43

Table 25:- Unauthorized network access 44

Table 26 :-Sniffing 45

Table 27:- Hacking 46

Table 28:-Data interception during file upload 46

Table 29; - Insider threat 47

Table 30:- Phishing 48

Table 31:- Malware program 48

Table 32:- Network security analysis 49

Table 33:- Port scanning 50

Table 34:- Vulnerability scanning 50

Table 35:- Physical security check on IT assets 51

Table 36:- Data analysis 51

ABBREVIATIONS/ACRONYMS

ACL	Audit Command Language
ATM	Automated Teller Machine
BC	Business Continuity
CAAT	Computer-Assisted Audit Tools and Techniques
CEO	Chief Executive Officer
CIA	Certified Internal Auditor
CIAO	Chief Internal Audit Officer
CISA	Certified Information System Auditor
CISM	Certified Information Security Manager
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of The Tread Way Commission
DR	Disaster Recovery
INSA	Information Network Security Agency
IS	Information System
ISACA	Information Systems Audit And Control Association
IT	Information Technology
ITAM	Information Technology Asset Management
NBE	National Bank of Ethiopia
OFAG	Office of the Federal Auditor General
PIN	Person Identification Number
POS	Point Of Sale

ABSTRACT

The main purpose of this study was to assess practice of information technology audit and fraud detection on commercial banks in Ethiopia. A descriptive type of research design was used and data were collected from all IT audit employees that are working in internal audit department of each banks. To achieve the objective of the study, questionnaire was used to gather data from IT auditors of various commercial banks in Ethiopia. The target population includes 64 IT audit personnel. The quantitative data were analyzed by employing appropriate techniques of descriptive statistics using SPSS software tool. The result of the study revealed that all commercial banks in Ethiopia had conduct IT audit. There were also faced different challenges. IT related frauds were existed on commercial banks in Ethiopia. The study recognized that there are common IT audit approaches used to detect IT related frauds. Based on the findings the commercial bank found in Ethiopia top-level management suggested to gives more emphases towards the IT audit process. In order to achieve their job in effective and efficient manner they support them, give attention consistently and reply the request as soon as possible and also the study suggested that an appropriate program was given for training and developing IT audit staff.

Keywords: IT Audit, IT related frauds, IT fraud detection

CHAPTER ONE

1. INTRODUCTION

The internal audit function is an important function that has been shown to add value and reduce detected errors by external auditors. Its objectives are to improve the effectiveness of risk management, control, and governance and it is considered an important governance tool to protect corporations from internal criminal behavior (Nestor 2004). Further, the professional literature suggests that internal audit is a vital tool in fraud detection when assets are misappropriated by employees or outsiders (Belloli, 2006).

The value of internal control is apparent in both preventing and detecting fraud as prevention is better than cure. A weak internal control creates opportunities for fraud and about half of all frauds occur in the financial area (Belloli, 2006). Internal control system has four broad objectives; those are to safeguard assets of the firm; to ensure the accuracy and reliability of accounting records and information; to promote efficiency in the firm's operation; and to measure compliance with management's prescribed policies and procedures. The effectiveness of internal control depends largely on management integrity.

IT plays a vital role in modern banking industry across the world. The banking industry in Ethiopia is one of the rapidly growing sectors of the country’s economy. In addition, the banking service has also dramatically changed from manual operation to the technology supported system which then brought the industry and customers to national and global presence anywhere-anytime (Patrick, 2011). In the light of computerization opportunities available across the world, organizations have been increasingly relying on the automation of their activities and information management (Panwar,et al, 2014)and the use of information Technology (IT) within the organizations has become increase significantly (Veerankutty & Mahzan, 2010).

Due to a pervasive and steadily growth of information and communication technology, world’s banking industry is entering into new phenomena of unprecedented form of competition supported by modern information and communication infrastructure. Currently, commercial banks and information technology products are two sides of a coin which cannot be separated. In order to deliver quality customer service and to stay competitive in the market, banks have to adopt information technology products and upgrade their service quality. Information technology investments in banks made to enhance better customer service; such as core banking software, Electro-banking like POSs, ATMs, mobile banking, internet banking and also any software and hardware used on daily activists of the bank (Rahel, 2016).

Information technology (IT) has become an effective and indispensable tool in modern business (Siew, et al, 2017). On the other hand, it has also brought with it an increasing range of IT frauds, vulnerabilities and threats of the automated business environment and associated organizational costs have increased tremendously along with new risk factors such as data loss due to vulnerabilities of network, the danger of tampering with data by insiders and outsiders is much higher in IT systems.

The reliability of computerized data and of the systems that process, maintain and report these data, protecting the organization’s assets and data, and ensuring efficient operations are a major concern and part of the role of information technology (IT) audit (Singleton, 2014).

1.1 STATEMENT OF THE PROBLEM

Benefits of IT together with customer expectations have made banks to integrate IT into their everyday activities. Thus banks have tended to rely heavily upon IT which has placed it amongst the most critical components that determine the survival of the business in the market place. IT failures would then be catastrophic and hence a major concern. In view of this, IT auditing has become very critical. The banking industry is heavily reliant on technology to carry out its operations. This has resulted in diverse delivery channels that have increased the options offered to customers to carry out their transactions with ease, speed and convenience. These developments have however led to various challenges such as dependence on vendors due to outsourced IT services, multiplicity and complexity of systems, insider security threats, as well as more exposure to fraud risks (RBI, 2011).

The IT auditor is faced with different tasks of providing audit assurance on IT systems as well as adding value through early detection and prevention of frauds. The audit tools available combined with deductive reasoning can enable the IT auditor to be more proactive in detecting fraud.

(Alemayehu, 2016), in his case study on Ethiopian budgetary public sectors, argue that there is insufficient auditors ‘competence and independence problem toward the usefulness of internal audit work to detect and prevent fraud.

Fraud skills and fraud awareness addressing what auditors need to know to detect and handle fraud. This knowledge gap allows fraud to occur and go undetected. (Jonathan Adegoke1, K. S., 2013), states that internal auditors must have a superior level of theoretical knowledge and practical experience in order to successfully accomplish their role. They concluded that auditors must know the possible fraud schemes and scenarios that are specific to an organization's field of work and be able to recognize the signs of a possible fraud scheme. According to (Daniela, 2014)argued the role of the internal audit include a varied set of responsibilities: supporting the management in establishing auditable anti-fraud mechanisms; facilitating the assessment of fraud and reputational risks at the level of an organization and its business process; assessing the connections between fraud risks and internal controls; auditing frauds; supporting the specialists in fraud investigation; supporting the efforts to rectify deficiencies; and reporting to the audit committee the problems regarding anti-fraud mechanisms, fraud and reputational risks assessment, or fraud cases and suspicions.

According to (Daniela, 2014)studies on fraud, internal audit department should be given the authority to handle their tasks and it is vital that they are independent of management in order to carry out their duties without 'fear or favor' in fraud fighting. Fraud risk assessment is a tool that assists internal auditor in systematically identifying where and how fraud may occur and who may be in a position to commit fraud. According to the National Standard on Audit 240 'Fraud and Error' (NSA 240), when planning the audit, the auditor must assess the risk related to the fact that fraud and error can lead to significant misrepresentations in the financial reports and he must request from the management information about any substantial fraud or error discovered.

The research that was conduct before has extensively examined the determinant factors that influence internal audit effectiveness such us top management support, organizational setting, quality of audit work, organizational independence and there is a lack of a wide IT audit research which evaluates the practice of IT audit and fraud detection regarding to banking sectors in Ethiopia.

In case of Ethiopia, reviewing the internal audit literature shows that no direct research on the practice of IT audit and fraud detection in banking sectors. As the result, the researcher is motivated to assess the practice of IT audit and fraud detection on commercial banks in Ethiopia.

1.2 RESEARCH QUESTION

- What are IT audit focus areas conducted on commercial banks in Ethiopia?
- What are the challenges faced in conducting IT audit assignment?
- What are IT related fraud occurred on commercial banks in Ethiopia?
- What are IT audit fraud detection approach against IT related frauds?

1.3 OBJECTIVE OF THE STUDY

1.3.1 GENERAL OBJECTIVE

The general objective of the study is to assess the practice of IT audit and fraud detection on commercial banks in Ethiopia.

1.3.2 SPECIFIC OBJECTIVE

The study has the following list of specific objectives.

- Assess the practice of IT audit focus area on commercial banks in Ethiopia.
- Identify the challenges faced in conducting IT audit assignment.
- Assess IT related frauds occurred on commercial banks in Ethiopia.
- Assess the practice of IT audit fraud detection approach against IT related frauds.

1.4 SIGNIFICANCE OF THE STUDY

The National Bank of Ethiopia has a regulatory function over the banking industry in Ethiopia. National bank of Ethiopia as part of stabilizing and enhancing efficiency in the banking sector and hence the findings from this study would be of interest to the NBE.

Government agencies and institutional bodies like the Ministry of innovation and technology of Ethiopia and Information Network Security Agency (INSA) would be interested in knowing the extent of IT related frauds in the banking industry. This would be a useful to implement strong controls framework and making policy decisions relating to IT fraud in Ethiopia. Implementation of the IT policy and the e-government strategy documents would require a functional e-commerce network as it involves transfer of assets and money. The required IT compliance in the banking sector can only be verified through IT auditing since most systems has integrated technology and hence the findings of the extent of the practice are useful.

The study documented the challenges faced in IT audit would make the auditors to be more prepared as they plan their audits in banks in Ethiopia. The study shall also add to the body of knowledge for researchers.

1.5 SCOPE OF THE STUDY

This study was assessed practice of IT audit and fraud detection on all commercial banks in Ethiopia. Accordingly, seventeen banks are selected for the study. From the total banks selected for the study, sixteen of them are private commercial banks and one is government banks.

1.6 LIMITATION OF THE STUDY

The major challenges the researcher faced, that might have an implication on the overall result of the study includes firstly, at a local level, there were no empirical research works aimed at investigating the practice of IT audit in fraud detection.

1.7 STRUCTURE OF THE THESIS

The research report was presented in five chapters.

Chapter one presented introduction, statement of the problem, research questions and objectives of the study, significance of the study, scope and structure of the study.

Chapter two summarized the result of in depth literature review relevant to the study. It focuses on the theoretical aspect and empirical findings.

Chapter three discussed the type and design of the study, provide information about the study participants, sources of data, data collection tools, the procedure of data collection and data analysis technique employed to arrive on the research findings.

Chapter four presented the finding of the study, analysis and interpretation of the findings. It also briefly state whether the result of this study conforms or negate with the literature review results.

Chapter Five deals with the brief summary of the findings of the research, conclusions drawn from the analysis and recommendation thereof.

CHAPTER TWO

2 LITERATURE AND EMPIRICAL REVIEW

2.1 THEORETICAL LITERATURE

Most businesses, private or public, profit or not-for profit, are increasingly dependent on information technology and it has also impacted the business environment in three significant ways: IT has increased the ability to store, capture, analyze, and process tremendous amounts of information, IT has significantly impacted the control process and IT has also impacted the auditing profession in terms of the skills required to perform an audit and the knowledge required drawing conclusion (Wagner, 2011).

The importance of information technology, the need to derive more value from IT investments and manage IT-related risks is increasing. Business executives and managers are taking ownership and making organizational changes to create a more effective structure for overseeing and monitoring IT-related goals and issues. IT auditors should have expert knowledge regarding IT risk and controls to provide assurance to management (Mengistu, 2016).

The extensive use of IT in business today has had a major impact on the audit profession too. Keeping pace with this technology and ensuring that it exists within a secure and controlled environment is one of the key challenges facing the audit profession (Komneni, 2008).

In addition, IT presents risk factors that are unique to accounting, auditing and systems. That is, IT itself brings risk to the entity regarding its systems, business processes and financial/accounting processing. That risk is unique to IT and without IT being present, that risk would not exist, at least not to the same level. It takes a professional, such as an IT auditor, to identify and assess the inherent risk associated with IT. Those risk factors include systems-related issues, such as systems development, change management and vulnerabilities, and other technology-specific factors (Singleton, 2014).

IT auditing began as Electronic Data Process (EDP) Auditing and developed largely as a result of the rise in technology in accounting systems, the need for IT control, and the impact of computers on the ability to perform assurance services. When compared to auditing as a whole IT auditing has had a relatively short yet rich history and remains an ever changing field (Nkwe N. , 2011).

IT Auditors evaluate the effectiveness and efficiency of IT controls in information systems and related operations to ensure they are operating as intended (ISACA, 2010). The IT audit activity provides assurance around all-important risks, including those introduced or enabled by the implementation of IT. So due to the increased reliance of business operations on IT and new regulations regarding the assurance of IT for those operations, information technology auditioning has grown rapidly (Stoel, et al, 2012).

2.1.1 DEFINITION OF IT AUDIT

Today the global economies are more dependent on information technology and the IT related risks have more impact on the business and required for strong IT controls for business operations, this calls for IT audit. (Stoel, et al, 2012).

"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" (Harb, 2012); (Siew, et al, 2017), (Mengistu, 2016); (Alraja & Lomiam, 2013); (Axelsen, et al, 2011).

IT auditing is the process of gathering and evaluating evidence based on which one can evaluate the performance of IT systems to determine whether the operation of information systems in the function of preserving the property and maintain data integrity (Mengistu, 2016). The primary role of an IT audit is to ensure the integrity of an organization's information systems (Harb, 2012). Identifying and addressing risk is one of the business most important issues and IT is central to any organization. The IT audit ensures that these risks are addressed quickly and carefully (Björklund, J. and Joelsson, R., 2015).

One aspect of conducting IT audits is the discovery of irregular acts, i.e. intentional violations of policies or regulations, or unintentional breaches of the law (Merhout, J., and Havelka, D, 2010).

In a complex and dynamic business environments where IT becomes significant to the organizations, the role of the internal audit function changes from a traditional one focuses on accounting and financial control to a more strategic one which focuses on risk management and corporate governance, the overall corporate governance applies to IT governance efforts too to assist all employees and business functions including IT and its Governance of the organization to give assurance, evaluations and recommendations (Mengistu, 2016).

2.1.2 THE NEED FOR IT AUDITING

Computers play a vital role in assisting the organization to process data and to make decisions, it is important that their use should be controlled, because the rapidity of change and amount of resources invested in IT from time to time makes the activities complex to the management of IT (Mengistu, 2016) and the costs of errors and irregularities that arise in these systems can be high. Not only controlling their use, the way they are utilized and their impact on the overall objectives of an organization have to be evaluated (OFAG, 2017). This calls for the requirement of the auditor to become involved in supporting and helping implement corporate governance in IT and management (Mengistu, 2016).

The demands of IT auditing highly increase in recent years as a result of the accounting scandals and increased regulation. IT auditing adds security, reliability and accuracy to the information systems. ISACA stated that the IT auditor can help organizations implement control structure processes such as Control Objectives for Information and Related Technology (COBIT), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and International Organization for Standardization (ISO) standards 9000, 9001, 17799, and their amendments (Walker, 2015).

IT audits are important organizational processes that add value to the organization because they have given an assurance on the integrity, reliability and quality of the information produced by the organization’s information systems (Siew, et al, 2017). IT audit is needed to assure that the information gathered through systems is controllable, secure and functional. The IT auditor plays an increasingly important role in helping companies manage and respond to risks (Björklund, J. and Joelsson, R., 2015).

Moreover, organizations with the increased reliance on computers to perform their daily transactions and with the advanced threats and risks associated with new technology, the organizations management needs assurances that the internal controls governing the business computer/system operations are adequate (Harb, 2012).

All industries should perform an IT audit, but it is critical for banks and financial institutions and also according to regulations, required to develop an information technology audit program to support its information technology infrastructure, to keep non-public customer information secure, and to conduct a risk-based audit on an annual basis (Lovaas, 2012)

IT audit provides more reliable and more accurate information on IT asset protection, data integrity maintenance. The final result of IT audit is not just a report but its effects and a timely implementation of recommendations and corrective activities (added value) with the purpose of implementation business goals of the company in its entirety (Rotim & Komnenić,, 2010).

2.1.3 IT AUDIT OBJECTIVES

The purpose of IT auditing is to assess whether or not an information system is achieving stated organizational objectives and to ensure that the system is not creating an unacceptable level of risk for the business (Rahman, 2014). IT audit also ensure that the IT resources allow organizational goals to be achieved effectively and use resources efficiently (Panwar,et al, 2014). Moreover the purpose of an IT audit is also to discover where improvements can be made, and to ensure that the company is in compliance with internally and externally mandated laws and regulations (Lovaas, 2012).

The objective of conducting an IT audit is to evaluate an organization computerized information system in order to ascertain whether the information system produces timely, accurate, complete and reliable information outputs, as well as ensuring confidentiality, integrity, availability and reliability of data and adherence to relevant legal and regulatory requirements (Kozlovs, D. et al, 2015), (Lovaas & Wagner, 2012)

- **Confidentiality**: refers to 'the protection of sensitive information from unauthorized disclosure. Management needs assurance of the organization ability to maintain information confidential, if confidentiality compromises could lead to significant public reputation harm.'
- **Integrity**: refers to 'the accuracy and completeness of information as well as to its validity in accordance with business values and expectations. It provides assurance to management that the information produced by the organizations information systems can be relied and trusted upon to make business decisions.'
- **Availability**: relates to 'information being available when required by the business process now and in the future and also cancers the safeguarding of necessary resources and associated capabilities. It gives assurance that the information they need for decision making is available when required'

- **Reliability**: refer to 'the degree of consistency of a system or the ability of a system to perform its required function under stated conditions. IT audit provides assurance that the system consistently operates and performs its stated function as expected.'
- **Compliance with Legal and Regulatory Requirements**: 'Compliance deals with complying with those laws, regulations and contractual obligations to which the business process is subject."

2.1.4 IT CONTROLS

IT controls are designed to meet control objectives related to Information Security requirements. The core objectives, often referred to as C-I-A ,Confidentiality: Protects sensitive information from being viewed by unauthorized users such as Financial Data, Credit Card Numbers, etc., Integrity: Protects the integrity of critical IT resources like Hardware, Software, data repositories, Availability: Ensures that critical IT resources (i.e., hardware, software, and data) are available when needed (William, B. et al., 2013). (Richard et al., 2010)

Internal controls include risk management, compliance with internal procedures and instructions and with external legislation and regulations, periodic and ad hoc management reports, progress checks and revision of plans and audits, evaluations and monitoring (Panwar,et al, 2014)

Controls in a computer information system reflect the policies, procedures, practices and organizational structures designed to ensure the protection of the organization's assets, the accuracy and reliability of its records, and the operational adherence to the management standards (Panwar,et al, 2014).

IT controls provide for assurance related to the reliability of information and information services and used to help mitigate the risks associated with an organization's use of technology (Richard et al., 2010).

IT controls are used to mitigate the risks associated with in the IT environment and application systems and classified in to two categories: General IT Controls and Application IT Controls (Panwar,et al, 2014).

IT General Controls are the foundation of the IT Control structure and concerned with the general environment in which the IT systems are developed, operated, managed and maintained. These are designed to manage and monitor the IT environment that affect all applications and which focus on the management and monitoring of IT. General IT controls are applied to all systems components, processes, and data for a given organization or systems environment. The objectives of these controls are to ensure the appropriate development and implementation of applications, as well as the integrity of program and data files and of computer operations (Panwar,et al, 2014). The most common controls are: Logical access controls over infrastructure, applications, and data, System development life cycle controls, Program change management controls, Physical security controls over the data center, System and data backup and recovery controls and Computer operation controls (Panwar,et al, 2014), (Richard et al., 2010).

Application IT Controls are specific controls unique to each application systems. They include controls that help to ensure the proper authorization, completeness, accuracy, and validity of transactions, maintenance, and other types of data input, encryption of data to be transmitted, processing controls, etc. These controls are used to provide assurance (primarily to management) that all transactions are valid, authorized and recorded (Panwar,et al, 2014), (Richard et al., 2010). The objective of application controls is to ensure that: Input data is accurate, complete, authorized, and correct; Data is processed as intended in an acceptable time period; Data stored is accurate and complete; Outputs are accurate and complete; record is maintained to track the process of data from input to storage and to the eventual output (Bellino, 2010)

2.1.5 AREAS COVERED THROUGH IT AUDIT

2.1.5.1 IT GOVERNANCE

IT Governance is the overall framework that guides IT operations and an integral part of the enterprise governance in an organization to ensure that the IT investments and activities are aligned and meet the business objectives (Panwar,et al, 2014).

The objectives of IT governance are IT is aligned with the business, IT enables the business and maximizes benefits, IT resources are used responsibly, and IT risks are managed appropriately. IT auditing is major tool for IT governance, the IT auditors are involved in giving assurance that each of these objectives met. For easy IT auditing adoption, employees who have business and IT skills are needed (Nkwe N. , 2011)

2.1.5.2 PHYSICAL ACCESS CONTROL

Physical access control is the restriction of access to a physical space within the business or organization. This type of access control limits access to rooms, buildings and physical IT assets. In addition, physical access control keeps track of who is coming and going in restricted areas.

The objective of physical and environmental controls is to prevent unauthorized access and interference to IT services. In meeting this objective, computer equipment and the information they contain and control should be protected from unauthorized users. They should also be protected from environmental damage, caused by fire, water (either actual water or excess humidity), earthquakes, electrical power surges or power shortages. The entity's IT security policy should include consideration of physical and environmental risks (James A.Hall, 2011)

2.1.5.3 LOGICAL ACCESS CONTROL

Logical access controls are those controls that either prevent or allow access to resources once a user's identity already has been established. Once a user is logged in, they should have access only to those resources required to perform their duties (Collins, 2013).

The objective of logical access controls is to protect the applications and underlying data files from unauthorized access, amendment or deletion. The objectives of limiting access are to ensure that: users have only the access needed to perform their duties, access to very sensitive resources such as security software program, is limited to very few individuals, and employees are restricted from performing incompatible functions or functions beyond their responsibility (James A.Hall, 2011).

2.1.5.4 IT ASSET MANAGEMENT

IT asset management (ITAM) comprises practices and strategies for overseeing, managing and optimizing company-owned IT systems, hardware, processes and data. As part of an ITAM strategy, IT departments implement, track and maintain IT assets, and assess whether those IT assets require optimization, can be replaced with a less expensive option or be upgraded to a newer technology (White, 2019). The objectives of IT Asset Management is to provide the organization with a deep knowledge of its information systems to use this information for the identification and rapid resolution of problems (White, 2019).

2.1.5.5 DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

IT disaster recovery plans provide step-by-step procedures for recovering disrupted systems and networks, and help them resume normal operations. The goal of these processes is to minimize any negative impacts to company operations. The IT disaster recovery process identifies critical IT systems and networks; prioritizes their recovery time objective; and delineates the steps needed to restart, reconfigure, and recover them. A comprehensive IT DR plan also includes all the relevant supplier contacts, sources of expertise for recovering disrupted systems and a logical sequence of action steps to take for a smooth recovery (James A.Hall, 2011). The objective of DR and BC plan is to limit risk and get an organization running as close to normal as possible after an unexpected interruption.

2.1.5.6 DATA BACK UP AND RESTORATION

Backup and restore refers to technologies and practices for making periodic copies of data and applications to a separate, secondary device and then using those copies to recover the data and applications and the business operations on which they depend in the event that the original data and applications are lost or damaged due to a power outage, cyberattack, human error, disaster, or some other unplanned event. The objective of the data backup is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human caused event, such as a malicious attack (virus or malware), or accidental deletion of data (ISACA, 2010)

2.1.5.7 DATA PROTECTION AND PRIVACY

Data privacy, also called information privacy, is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties (Rouse, 2016). The objective of data protection and privacy is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent (Wonde, 2014).

2.1.5.8 IT APPLICATION CONTROL

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 that all transactions are valid, authorized, and complete and recorded. The objectives of IT application controls are to ensure the completeness and accuracy of records, as well as the validity of the entries made to each record, as the result of program processing (James A.Hall, 2011).

2.1.5.9 NETWORK SECURITY

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Confidentiality, integrity and availability of network and data is the main objective of network security. (Anchugam & Thangadurai, 2018).

2.1.6 CHALLENGES FACED IN CONDUCTING IT AUDIT

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

Budget constraint is usually cited as a major factor limiting the implementation of successful and comprehensive IT audit among many developing countries. The level of deployment of IT in itself is limited due to the same reasons and hence subsequent verification of the integrity of the IT systems through an audit is also less applied (Sandra Senft, Frederick Gallegos, and Aleksandra Davis, 2012).

Infrastructure (Cabling, Data Center Facilities) Hardware (Server, Desktop, Laptop, Storage) pose a major challenge to IT auditors. Testing of the efficiency, compliance of defined standards, regulation requirements demand that the auditors be well rounded in their skill. Technical skills in networks implementation, maintenance policies, operating systems and administrations as well as knowledge about systems applications and development become necessary if the auditor to present a fair evaluation of the company's IT infrastructure and systems People have a culture of assuming that, if a system has been working well then there is no need to change. Technological advancement has however led to explosion of new threats to IT based systems and hence the need for continuous testing against most recent standards and benchmarking the IT systems against global standards (James A.Hall, 2011)

Low competency of use of IT auditing tools among the IT auditors results to limited application of these tools in IT audits. Some of the packages require competent programmers for example sequence query languages for optimum use. These skills are not commonly available among the traditional auditors and hence posing a major challenge to effective IT auditing (Champlain, 2012).

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

Disaster Recovery and Business Continuity is an important component of IT auditing. In many businesses Disaster Recovery Planning is a theory rather than practice. In most cases, some of the elements of the DR planning are not thoroughly tested, there is no simulation of disaster and hence when a catastrophe strikes there is very little continuity of business operations (Ndulu, 2004).

IT Security is of critical importance and should be a consideration to perform an explicit IT Security Audit. Information security has many elements most of them highly technical and requiring specialized skills not commonly available among many audit teams of many companies. This is an obvious challenge faced in IT audits in many developing countries (Ndulu, 2004).

2.1.7 DEFINITION OF FRAUDS

According to the Institute of Internal Auditors International Professional Practices Framework (2009) defines fraud as, "Any illegal act characterized by deceit, concealment, or violation of trust. Frauds are perpetuated by parties to obtain money, property or services; to avoid payment, or loss of services; or to secure personal or business advantage." It should be noted that frauds generally impacts a bank by causing financial, operational or psychological loss (Bhasin, 2015). The Association of Certified Fraud Examiners (ACFE) defines fraud as "the use of occupation for personal enrichment through deliberate abuse of employing organization's resources or assets" (Abdallah, 2016).

(Wikipedia, 2012), defines bank fraud as whenever a person knowingly executes, or attempts to execute, a scheme or artifice to defraud a financial institution; or to obtain any of the moneys, funds, credits, assets, securities, or other property owned by or under the custody or control of, a financial institution, by means of false or fraudulent simulations, representations, or promises (Wikipedia, 2012).

2.1.8 IT RELATED FRAUD

The banking industry is heavily dependent on technology to carry out its operations, and as such, banking business and technology cannot be discussed in isolation (Julia M, 2013). Diverse delivery channels have immensely increased the options offered to customers to carry out their transactions with ease, speed and convenience. These developments have led to various challenges such as dependence on vendors due to outsourced IT services, multiplicity and complexity of systems, insider security threats, as well as more exposure to fraud risks (Chakrabarty, 2013).

According to (Goldmann, 2009), the followings are common IT related frauds exists in banking sector.

A. **Input transaction manipulation** schemes.

- ***Extraneous transactions***; - these are illegal transactions initiated by a trusted insider, such as unauthorized billing transactions that result in disbursement of company funds to the perpetrator or a shell company he or she controls. These frauds can also involve manipulating the organization' s computer data pertaining to one or more customers, vendors, products, accounting entries, salespeople, and so on that the perpetrator exploits at a later time.

- ***Failure to enter transactions***: -this is a common technique in many billing schemes. Examples: A purchasing associate who is perpetrating a billing scheme can intentionally prevent a false invoice from being entered into the payments system or an employee responsible for accounts receivable can neglect to credit an account when payment is received

- ***Transaction modification***: -also common in billing schemes or collusion, these involve fraudulently increasing or reducing amounts charged to a particular account.

- ***Misuse of adjustment transactions***: -computer systems for legitimately correcting accounting errors or to record adjustments to inventory loss or spoilage can be abused by employees with access to such systems by falsifying entries to cover up outright theft or more elaborate billing schemes.

B. **Unauthorized program modification schemes**: - this category of computer generated insider schemes typically involves making unauthorized changes to automated payment or accounting software programs. A common form of this crime involves programming the system to execute high numbers of mini frauds such as rounding of numbers, fraudulently adding service charges, or diverting amounts of money so small as to fall below the radar of internal controls on accounts owned by the fraudster.

- ***Processing undocumented transaction codes***: - by manipulating the payments system to accept undocumented, false transaction codes for small transactions in situations where controls are absent, the fraudster can program the system to process fraudulent transactions that are entered directly by the perpetrator or by the computer via unauthorized programming changes

- ***Balance manipulation***: -here a dishonest internal computer programmer alters specific programs in a way that fraudulently forces account balances, in order to conceal embezzlement or other types of fraud that would otherwise be detectable by auditors.

- ***Lapping schemes***: - an insider with authorization to utilize the organization’s automated accounting system can steal incoming payments and credit them to his or her own account and then manipulate the system to fraudulently credit the intended payee ’ s account with a payment subsequently received from another account. The process is repeated until, due to slipup in timing or sharp auditing, the scheme is detected.

- ***Fraudulent file modifications***: - these crimes involve secretly changing account status through basic computer programming. Examples: Opening a fraudulent new account to receive automatic payments from payroll, retirement, unemployment, or welfare systems, destroying records of a fraudulent account, or fraudulently increasing a credit limit on a revolving credit line.

C. **File alteration and substitution schemes**.

- ***Accessing a live master file***:- the internal fraudster accesses the file and, using a specially written program or a general retrieval program, makes fraudulent adjustments to the file, such as a Vendor Master File, by modifying account balances, altering a payee, changing supplier addresses, adding bogus vendors, and so on.

- ***Substitution of a dummy version of a real file***: - the fraudster initiates the scheme by obtaining access to the master file and then uses a special computer program to run the legitimate master file in order to create a duplicate. However, the duplicate has a few modifications when it is substituted for the legitimate file, thereby enabling the fraudster to hide fraudulent transactions that would otherwise be detected.

With these IT growth and development, fraud techniques have also evolved over time, and fraudsters are now targeting computer networks to perform fraud. In a bank, frauds can either be done by an insider, an external party or both parties can collude to defraud the bank. Insider threats are a big threat since they have access to information and assets and can easily pounce on vulnerabilities. External threats receive a lot of attention due to their frequency, magnitude or complexity and they include physical security breaches, hacking attempts, system sabotage amongst others (Mulwa D., 2012).

Other ways to commit fraud include sniffing, which allows the criminal to see plain text login credentials and confidential information transferred over networks; malware program which hackers can use to obtain credentials that can facilitate access to confidential information. Phishing attacks pull victims to a website masquerading as the legitimate web page. This form of attack affects the internet-banking channel of service delivery. A malware program known as root kit is usually accompanied by key loggers to capture sensitive information such as log-in credentials (Launius S.M., 2010).

(Aeran, 2010)has further reviewed the different types of security threats that an organization may have to face, and this includes; theft of intellectual property and an organization’s confidential information, for instance extracting a list of high net worth customers and selling them to competitors for commercial gain; password cracking and getting users passwords through illegal installations like key loggers in order to carry out transactions through identity theft. Criminals commit frauds such as phishing, database and server hacking, network attacks, cross site scripting, card cloning, obtaining confidential information through social engineering and insider threats, that may result in financial and reputational loss.

Online banking is designed mostly for the consumer and furthermore for banks to reducing the cost of operations. Phishing is the most common online banking fraud and the aims is to gather personal information such as banking logins, PIN, bank account number, and credit card numbers. The typical phishing scam involves an e-mail that appears as though it came from a reputable and known service institutions or company. The e-mail appears to be legitimate and the actual one. The message generally indicates that, due to problems in the bank such a database updates, problem occurred in server, security/identity theft concerns, the recipient is required to update personal data such as passwords, bank account information, driver's license numbers, social security numbers, Personal Identification Numbers (PIN), and so forth. The e-mails include warning to the users that failure to immediately provide the updated information will result in suspension or termination of the account (Singh. N.P, 2010). Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware (Wikipedia, 2012).

2.1.9 IT AUDIT DETECTION APPROACHES AGAINST IT RELATED FRAUDS

The IT auditor must possess essential skills, which include an understanding of general computer controls, data analytics, knowledge of the system infrastructure and excellent risk expertise. General computer controls involve understanding the internal controls around IT systems and applications and the review of controls that mitigate the risk of threats to the systems. Data analytics skill requires the IT auditor inspect, clean, transform and model data and highlight useful information and suggest recommendations. The knowledge about networks, hardware, operating systems, databases and applications is essential for the IT auditor in order to assess the risks and ensure that they addressed appropriately (Julia, 2013).

Detective measures can be reactive or proactive. Most of the traditional fraud detection methods are reactive since they are initiated by tips or complaints, control overrides or other indicators that someone observes or hears (Albrecht, 2010). Instead of using reactive measures such as relying on whistleblowers and anonymous calls, the IT auditor should be more proactive by taking on a hands-on approach to fraud detection (Coderre D.G., 2010).The proactive approach requires the IT auditor to aggressively target specific types of frauds and look for indicators, symptoms or red flags (Albrecht, 2010)

The IT auditor, can use various statistical methods and tools in detecting fraud which includes Deloitte’s Statistical Techniques for Analytical Review (STAR) tool, which helps in the identification of abnormal patterns such as significant fluctuations on data, ACL for data analysis used for testing relevant transactions across all applicable business systems and applications (Coderre D.G., 2010). IT auditor should consider fraud vulnerability assessments while identifying fraud risk factors as part of IT risk assessment and audit process. The use of vulnerability scanners, penetration testing tools and operational and management controls when testing and evaluating the effectiveness of IT controls. Banks are therefore expected to implement tools and techniques that shall help support the procedure that the IT auditors will be performing to increase efficiency and effectiveness of the IT audit (Nkwe N. , 2011)

Customers are demanding the convenience of direct access to their data using their mobile devices, and banks are make available their IT infrastructure in order to launch self-service applications for opening new accounts, applying for loan, mortgages and other retail banking functions. However, distribution of information through the corporate banking network also introduces security risks in which network ports remain open to the Internet. As a result, the entire network exposed to external hackers to exploit in order to gain access to the internal network from which they can steal data. Hence, port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

Checking of physical security of IT assets is to safeguard information, equipment, IT infrastructure, facilities and all other banks IT assets. The physical security of IT assets can be broadly categorized based on the following criteria, security of IT asset location, human access control and environmental control. The place of the information asset room need to physical secured. It is always a good practice not to make known the location of server room to public.

IT auditors must enhance the use of Computer Aided Audit Techniques (CAATs), which may be used effectively in areas such as detection of revenue leakage, the assessment of control weakness and the monitoring of customer transactions for any abnormal patterns (Nkwe N. , 2011). Practices that need to be followed to enable early detection and prevention of fraud include review of new products and processes; creation of fraud awareness amongst staff and customers; enforcing know your employee/vendor procedures; ensuring there are adequate physical security on IT assets; ensuring that there are strict password account management practices; and ensuring there is proper segregation of duties and dual control is implemented.

To find vulnerabilities in a network, the IT auditor can use tools used for network surveying and scanning by probing an IP address or a range of IP addresses and gathering useful information such as the operating system used, the type of devise or the service being provided (Launius S.M., 2010). Network reconnaissance and port scanning reveals the potential holes in the network infrastructure, such as ports that are accessible, that can be used by criminals to launch an attack.

The IT auditor needs to also regularly review the IT strategy, policies and procedures covering areas such as the network architecture, procurement of hardware and software, processes of out-sourcing, in-sourcing and in-house development of solutions (Nkwe N. , 2011).

2.2 EMPIRICAL LITERATURE

The empirical study concerns previous academic research on the practice of IT audit in fraud detection and prevention. In this case, there are certain empirical studies undertake by different researchers related to the IT audit practice discussed in the following.

(Bzuwerk, 2018), conducted study on factors affecting IT audit quality in commercial banks in Ethiopia. The general approach of this research was an exploratory study in which a combination of quantitative and qualitative methods has been used to collect and analyze data. Based on extensive literature review, a research model was established which incorporates six factors that affect the quality of IT audit within commercial banks in Ethiopia. The six variables that are measured in this current study are: auditors' IT knowledge and competencies, auditors' IT control knowledge, target system complexity, audit procedure and methodology, auditing skills and resource availability. The findings of the study show that there is a positively significant relationship between IT Audit Quality and Auditors IT Control Knowledge, Target System Complexity, Auditing Skill, Audit Procedure and Methodology, Resource Availability and Auditors IT Knowledge and Competency. The researcher was asked the respondents to rank the critical once from the six factors. The result indicated that Auditors IT Knowledge and Competency ranked first, Auditors IT Control Knowledge ranked second, Audit Procedure and Methodology ranked third, auditing skill ranked fourth, Resource Availability ranked fifth and Target System Complexity ranked sixth. According to the result, the researcher concluded that Auditors IT Knowledge and Competencies, Auditors IT Control Knowledge, Audit Procedure and Methodology and Auditing Skill which were ranked by the respondents from one to four respectively are the most critical factors that affect IT audit quality. Resource Availability and Target System Complexity are the lowest factors that affect the Quality of IT Audit.

(Tariku, 2018), conducted study on assessment of information system audit in case of commercial bank of Ethiopia. Factors such as career and advancement, professional competence, quality of audit work, professional competency relationship between internal and external auditor and top management support. Both primary and secondary data are used the research used SPSS software and descriptive statistical tool such as tables, frequency, percentages, mean and standard deviation is used in analyzing the data collected.it is confirmed that career and advancement, professional competence, quality of audit work, professional competency, and top management support has negative influence, but relationship between internal and external auditor positive influence on information system audit processes. This is customizing to the current system audit providing appropriate programs for training and developing the system auditors by allotting some percentage of the total time of the work for continuing education and certification. Providing the information system audit process all the necessary support required from the top management give them independence; providing training and development programs to keep up to date in the field, and providing all the required physical resources.

(Julia, 2013), conducted study on the IT audit and fraud detection in commercial banks of Kenya, study focused on commercial banks in Kenya. The study tries to find to determine the extent of IT related fraud in Kenyan commercial banks, to establish the challenges faced during IT auditing by the IS auditor, to establish the countermeasures implemented in preventing fraud through IT auditing and to determine the relationship between IT auditing and fraud prevention. The study made use of the descriptive survey design. Questionnaires were used to gather data from IT auditors of various commercial banks in Kenya. Statistical methods such as mean, standard deviation, factor analysis and regression analysis were utilized to analyze the data collected from the respondents. From the findings, it was evident that banks had encountered IT-related fraud. As a result, IS auditors utilize different IT audit approaches and mitigation strategies in the detection and prevention of fraud and most of the respondents concurred, to a great extent, that there is a relationship between IT audit and fraud prevention.

(Nzuki, 2006), conducted study on survey of ICT on commercial banks of Kenya. As per (Nzuki, 2006), increased use of computer based- information systems, commercial banks have become more exposed to risks that could result into gross financial losses. This has resulted to increased demand for assurance to the management and other stakeholders that the business's ICT systems are operating as intended. The study was an exploratory survey targeting all commercial banks with operations in Nairobi. The design was appropriate considering that not much was known to make it possible to do a more advanced research. Data collection was done through a questionnaire. Of the 46 commercial banks targeted for the study, there were 38 fully completed questionnaires which represented an 82.6 % response. Data collected from the respondents was analyzed using various statistical tools and findings were found adequate to make inferences and generalization of the state of ICT auditing in commercial banks in Kenya. The study found that ICT auditing among Kenya's commercial banks faced numerous challenges. Poor assessment of threats and vulnerabilities was found to be the most challenging factor as well as the lack of awareness about ICT auditing by senior managers. Other major challenges were related to the complexity of ICT infrastructure and poorly defined compliance framework for Kenya. The concept of ICT auditing was hence found to be a newly emerging phenomenon and hence existing gaps and lack of standard ICT audit framework/guidelines was found to be a challenge especially among the smaller banks. In addition, the complexity of the ICT auditing exercise coupled to ICT being a highly technical field, ICT auditors required specialized skills which in most cases were not readily available among the conventional audit teams.

Generally, as the evidence above empirical studies were on the practice of IT audit, factors affecting IT audit quality and assessment of IT audit and fraud detection.

Based on the above theoretical and empirical evidence this study focuses on assessing the practice of IT audit and fraud detection on commercial banks in Ethiopia.

CHAPTER THREE

3. RESEARCH METHODOLOGY

3.1 RESEARCH DESIGN

A research design is a plan, structure, and strategy of an investigation so conceived as to obtain answers to research questions or problems. The plan is the complete scheme or program of the research. It includes an outline of what the researcher will do from writing the hypotheses and their operational implications to the final analysis of data (Kumar, 2011).

A traditional research design is a blueprint or detailed plan for how a research study is to be completed- operational zing variables so they can be measured, selecting a sample of interest to study, collecting data to be used as a basis for testing hypotheses, and analyzing the results (Kumar, 2011).

In this research, a descriptive research design was used. This study describes and assesses the practice of IT audit and fraud detection on commercial banks in Ethiopia. The descriptive study attempts to describe systematically a situation, problem, phenomenon, service, or program, or provides information about, say, the living conditions of a community, or describes attitudes towards an issue (Kumar, 2011). The descriptive study is used to explain the phenomena by associating with the statement and facts on the ground as they were aimed at explaining why the situation has happened. This gives a high degree of honesty and integrity in reporting the finding.

3.2 RESEARCH APPROACH

In this study, the researcher used quantitative method with emphasis on conducting questionnaire and analyzing the data by statistical software. Quantitative methods are research techniques primarily dealing with numbers and measurable features (Creswell, 2014).

3.3 RESEARCH POPULATION

Population is defined as the broad set of units of analysis that are under investigation, while element is the unit from which the necessary data is collected (Kothari, 2004). The target population of this study is IT auditors found in seventeen selected Ethiopian commercial banks which are in total 65. The selected banks have different number of IT auditors as indicated in the below table1.

Table 1:-Name of commercial banks in Ethiopia based on ownership

#	Name of the Bank	Ownership	# of IT/IS auditors found in the bank
1	ABAY BANK S.C.	Private	1
2	ADDIS INTERNATIONAL BANK S.C.	Private	3
3	AWASH INTERNATIONAL BANK S.C.	Private	6
4	BANK OF ABYSSINIA	Private	3
5	BERHAN INTERNATIONAL BANK	Private	2
6	BUNNA INTERNATIONAL BANK S.C	Private	4
7	COMMERCIAL BANK OF ETHIOPIA	Government	13
8	COOPERATIVE BANK OF OROMIA S.C.	Private	3
9	DASHEN BANK S.C.	Private	5
10	DEBUB GLOBAL BANK S.C	Private	2
11	ENAT BANK S.C	Private	3
12	LION INTERNATIONAL BANK S.C.	Private	2
13	NIB INTERNATIONAL BANK S.C.	Private	3
14	OROMIA INTERNATIONAL BANK S.C.	Private	3
15	UNITED BANK SHARE COMPANY	Private	4
16	WEGAGEN BANK S.C.	Private	5
17	ZEMEN BANK S.C.	Private	3
		Total	65

Source: **www.nbe.org.et**

3.4 SAMPLE SIZE

Because the total number of the participants was 65 which was not recommended to sample target population below 100; the researcher use total population of the study that is all IT auditors including managers found in 17 commercial banks of Ethiopia.

3.5 DATA COLLECTION

The data collection instrument used in this study is closed ended questionnaire which is design to identify and meeting the research objectives. This instrument chosen for data collection because of its suitability in having an ample time for the respondents concerned adequately fill the form. The questionnaire designed to include structured questions. Structured questionnaires are preferred for the ease of creating, coding and interpreting the addressed questions. The research questionnaires were adapted from previous study like (Tariku, 2018), (Bzuwerk, 2018), (Julia, 2013)and (Nzuki, 2006)modified according to the study needed. As (Kothari, 2004)said, structured questionnaires are simple to administer and relatively inexpensive to analyze. The structured questionnaires are reliable in that everyone in the sample will asked the same question and answers exactly the same way. It had its limitations in that it is hard to address complex issues and is difficult to know whether the respondent has understood the questions. The questionnaire contains closed ended questions. Choices questions are measure in Likert-Scales containing five choices, which ranges from No extent at all up to Very great extent: No extent at all (1), little extent (2), moderate extent (3), great extent (4) and very great extent (5).

3.6 DATA ANALYSIS AND INTERPRETATION

The data collected through the questionnaire were analyzed and present using descriptive statistics (frequency and percentage). Data analyses was conduct through descriptive statistics to give information about the demographic question and IT audit practice in detecting IT related frauds. Statistical Package for Social Science (SPSS) version 22 was used for data analysis. The collected data from questionnaires was screen and coded for completeness and accuracy and the response on each item put into specific ideas in a scientific way for easy analysis. To draw a meaningful conclusion, data was summarized and presented using appropriate table and figure format with frequencies, percentages for classifications of responses for easier understand and also for visual impression.

3.7 VALIDITY OF THE STUDY

Validity can be measured in the form of content and construct. Content validity is the assessment of how well the survey instrument items address the problem being investigated. Construct validity is an assessment of the constructs whether they measured the dependent variable or not (Lee & Kerlinger, 2011)

In order to assess the content validity of this research, OFAG IT audit experts evaluated the items of the survey questions. The feedback was collected for modification, correctness and reasonability aiming at increasing the questionnaires validity and clarity. Accordingly, the instruments were revised based on the subject matter experts' collected feedback.

3.8 RELIABILITY

Reliability measures internal consistency of the subjects in the survey items for example, if an object is measured multiple times using the same instrument, nearly the same result should be found each time with little or no measurement error (Lee & Kerlinger, 2011). Data reliability refers to the data collected by independent collector and if the same questionnaire is administered by another person will yield the same results or is chiefly concerned with making sure the method of data gathering leads to consistent results (Norman, G, 2003). Cronbach's coefficient alpha is broadly used by many researchers as criterion to assess the reliability of the scale. Cronbach's alpha is a model of internal consistency based on the average inter-item correlation (Norman, G, 2003).

For this study reliability analysis has been conducted using Cronbach's Alpha test to measure the reliability and internal consistency of the survey. The Cronbach's alpha coefficient (.954), (.854), (.928) and (.859) for IT audit focused area questions, challenges faced during IT audit questions, IT related frauds questions and IT audit fraud detection approach questions respectively. This indicated that the survey questionnaire is reliable since it is greater than 0.7 which is the minimal alpha value.

Reliability Statistics	
Cronbach's Alpha	N of Items
.954	8

Table 2:-Reliability of statistics for IT focused area questions

Reliability Statistics	
Cronbach's Alpha	N of Items
.854	7

Table 3: -Reliability of statistics for Challenges faced during IT audit questions

Reliability Statistics	
Cronbach's Alpha	N of Items
.828	8

Table 4: -Reliability of statistics for IT related frauds questions

Reliability Statistics	
Cronbach's Alpha	N of Items
.859	6

Table 5: -Reliability of statistics for IT audit fraud detection approach questions

Source: Reliability statistics analysis by SPSS 2020

3.9 ETHICAL CONSIDERATION

Ethics in research is very important because the research frame and circumstances need participations from all parties. Research conducted for academicals purpose only the respondents answer is protected, data protection, reciprocity and trust, affiliation and conflicts of interest no one can't be harm due their participation in research because of information system document is closed.

CHAPTER FOUR

4. DATA PRESENTATION ANALYSIS AND DISCUSSION OF RESULTS

This chapter presents and analyses the data collected from the various respondents for the purpose of the study. The findings and conclusions are based on this analysis. The chapter includes presentation of data and discussions of the respondent’s practice of IT audit in detecting IT related frauds in commercial banks of Ethiopia

4.1 RATE OF RESPONSE

The study had initially targeted 65 respondents and 60 respondents filled and returned their questionnaires thus constituting 92.31% response rate, while 5 of the respondents didn’t respond and never returned the questionnaires and constituted 7.69% non-response rate. This collaborate (Zikmund, 2003)assertion that a response rate of 50% is adequate, whereas a response rate greater than 70% is very good. This implies that based on this assertion; the response rate in this case of 92.31% was very good.

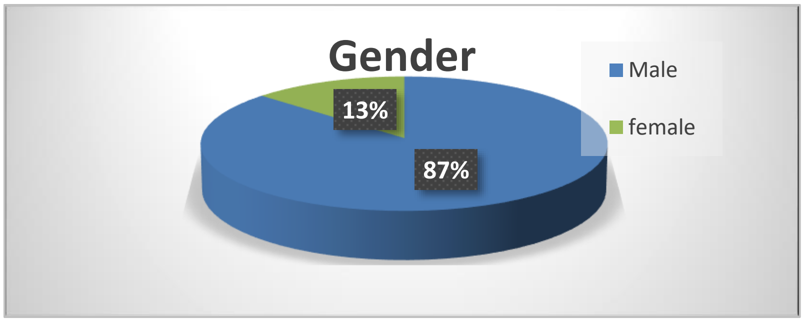
4.2 DEMOGRAPHIC CHARACTERISTICS OF RESPONDENTS

This section attempted to provide general characteristics of the respondents as captured by their responses in the current survey. The variables in these sections are gender, age, education level, work experience in the bank, IT/IS audit experience, level of professional certification and job position in the bank.

DISTRIBUTION OF RESPONDENTS BY GENDER

The research findings as reflected in table1 below, 87% of respondents were male and 13% were female. This is an indication that both genders were involved in this study and thus the finding of the study did not suffer from gender bias.

Figure 1: Distribution of Respondents by Gender



Source: Questionnaire Results, 2020

DISTRIBUTION OF RESPONDENTS BY AGE

The result of the findings as indicated in table 3 below, the dominant age groups in this study were age group between 25 to 35 years, which included 70% of the respondents. 25% were between 36 to 45 years, 5% of the participants were above 46 years old. This shows that the respondents are mostly young and energetic who are willing to learn and experiment new and emerging technologies.

Table 3:- Distribution of Respondents by Age

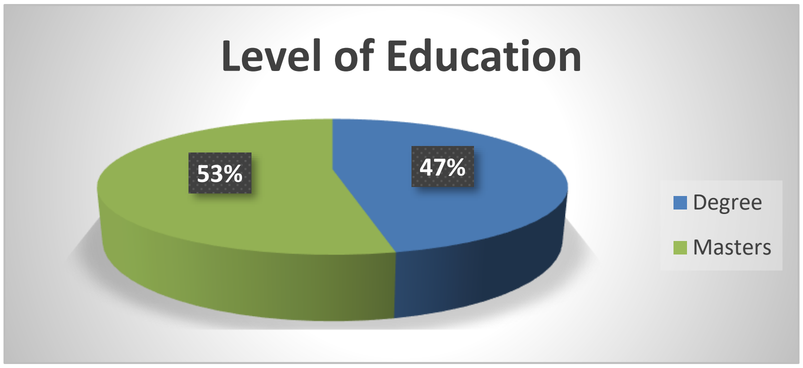
Age Group	Frequency	Percent
25-35	42	70%
36-46	15	25%
above 46	3	5%
Total	60	100%

Source: Questionnaire Results, 2020

DISTRIBUTION OF RESPONDENTS BY EDUCATIONAL LEVEL

The result of the study indicated in figure 2 below, 47 % of participants have a Bachelor's Degree and 53% have Master's Degree. Regarding academic qualification, as shown on table3 below, most of the respondents' were Bachelor's Degree holders. This shows that the majorities of IT auditors have the requisite qualification to perform their job and are ready to contribute towards the quality of IT audit and easily manage and detect frauds.

Figure 2:- :- Distribution of respondents by level of education



Source: Questionnaire Results, 2020

DISTRIBUTION OF RESPONDENTS BY WORK EXPERIENCE

The result of the findings relating to work experience in the company as indicated in table 4 below, 6.7 % of respondents work for less than 2 years, 35% between 2 to 5 years, and 33.3% between 6 to 10 years and the remaining 25% work for more than 10 years. The result shows that most of the respondents have working experience between 2 to 10 years (about 68.3%), this indicated that majority of the respondents had experience in the bank and this helps to IT auditors to know the business environment clearly.

Table 4:- Distribution of respondents by work experience

Bank Working Experience	Frequency	Percent
less than 2 years	4	6.7%
2-5 years	21	35%
6-10 years	20	33.3%
more than 10 years	15	25%
Total	60	100%

Source: Questionnaire Results, 2020

DISTRIBUTION OF RESPONDENTS BY IT AUDIT EXPERIENCE

Regarding to respondents' IT audit experience as indicated in table 5 below, 51.7% of respondents had less than 5 years, 33.3% had between 5 to 10 years, and the remaining 15% had more than 10 years IT/IS audit experience. The result shows that most of the respondents had IT/IS audit experience less than 5 years, this indicated that the IT audit is at infant stage and the audit is carrying out with less experienced IT auditors this may impact the quality of IT audit in detection IT related frauds.

Table 5:- distribution of respondents by IT audit experience

IT/IS Audit Work Experience	Frequency	Percent
less than 5 years	31	51.7%
5-10 years	20	33.3%
more than 10 years	9	15.0%
Total	60	100.0%

Source: Questionnaire Results, 2020

DISTRIBUTION OF RESPONDENTS BY PROFESSIONAL CERTIFICATION

Regarding to respondents professional certification as indicated in table 6 below, 3.3% of respondent had certification on IT Audit, 83.3% of the respondents had not professional certification and the rest 13.3% of the respondents had other professional certification The result shows that even if majority of IT auditors have 2nd degree, they had not taken professional certification in IT audit area and this indicated that the IT auditors lacks in expanding their knowledge and they are unable to coping technology changes easily, so that they are not perform IT audit assignment in efficient way.

Table 6:- Distribution of respondents by professional certification

Professional certification	Frequency	Percent
Certified IS Audit	2	3.3%
No Professional Certification	50	83.3%
Non-IT certificates	8	13.3%
Total	60	100.0%

Source: Questionnaire Results, 2020

4.3 IT AUDIT PRACTICE AND FRAUD DETECTING APPROACHES

This section provides information about IT audit practices in detecting IT related frauds on commercial banks in Ethiopia. From the responses of the respondent indicating in the below table 7, IT audit were conducted 80% by internal audit department staffs and the rest 20% of IT audit assignment conducted by external IT consultants. This indicates that conducting IT audit by internal staff can understand the bank operation easily, add value to the management and provides recommendations to improve the efficiency and effectiveness of procedures of the organization. The result is agrees with previous study that IT internal auditors analyze information systems and their operations through risk assessment, evaluation of internal control system in order to ensure the existence of prescribed risk mitigation control within company's information system to a minimum i.e. to an acceptable level (Komneni, 2008)

Table 7:- who conduct IT audit

Who Conduct IT Audit	Frequency	Percent
Internal Audit Department Staffs	48	80%
External IT consultants	12	20%
Total	60	100%

Source: Questionnaire Results, 2020

As indicating in the below table 8, regarding to period of conducting IT audit assignment, 17% of the respondents were said IT audit assignment conduct once in a year, 77% of the respondents said that IT audit assignment conducted continuously and the rest 7% said as per the risk assessment. This indicates that IT audit assignment conducted continuously. (Kozlovs, D. et al, 2015), stated that conducting IT audit continuously helps to detect errors and frauds easily and immediately because IT auditor checks continuously and also in a detailed manner.

Table 8 :- how often conducting IT audit

How often conducting IT Audit assignment?	Frequency	Percent
once a year	10	17%
Continuous	46	77%
Others	4	7%
Total	60	100%

Source: Questionnaire Results, 2020

On the subject of IT audit guidelines indicating in the below table 9, 70% of the respondents conduct IT audit assignment by referring banks Internal audit guideline, whereas the rest 30% of the respondents refer international guideline when conducting IT audit assignment. This indicates that IT auditors referred internal audit guideline which supports in conducting IT audit assignments. Literatures showed that to ensure the value of IT audits, organizations should set and implement a standard guideline for evaluating the quality of audits (Siew, et al, 2017). Adopting international standards and best practices helps to enhance the quality of IT audits. ISACA published a number of standards and auditing guidelines for IT auditors in different areas. Moreover, there are other relevant standards for IT auditors. ISO 27002, COBIT, and COSO are generally considered the IT audit models to follow for most organizations (Lovaas, 2012), (ISACA, 2010).

Table 9:- IT audit reference guideline

Where do the IT Auditors refer auditing guidelines for IT audit Assignment?	Frequency	Percent
Bank's Internal Audit Guideline	42	70%
international auditing guideline	18	30%
Total	60	100%

Concerning to providing final reports after conducting IT audit assignment indicating from the below table10, 22% of the respondents prepare technical report and the rest 78% of the respondents prepare moth technical and management final audit. This indicates that preparing of IT audit that holds both technical and management characteristic supports the management to understand as well as to implement the audit findings easily.

Table 10 :- types of IT audit report

What reports are provided after conducting IT audit?	Frequency	Percent
technical report	13	22%
Both technical and Management report	47	78%
Total	60	100%

Source: Questionnaire Results, 2020

About reporting structure of IT audit team indicating from the below table11, 13% of the respondents present their final report to board audit committee, 20% to CEO and the rest 67% to CIAO. This implies that, majority of the respondents' report their final IT audit report to CIAO. Hence the implementation and monitoring of IT audit recommendation is very weak.

Table 11:- reporting structure of IT Auditors

To Whom does the IT audit team report	Frequency	Percent
Board Audit Committee	8	13%
CEO	12	20%
CIAO	40	67%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.1 IT AUDIT FOCUSED AREA

The first objective of the study is to assess the practice of IT audit focus area on commercial banks in Ethiopia. The data collected was analyzed and presented on table and responses were measured using a five point Likert scale as follows; 1 represented no extent at all, 2 represented little extent, 3 represented moderate extent, 4 represented great extents and 5 represented very great extent. To consolidate and give presentation of the data, the study used the statistical functions of frequency and percentile.

4.3.1.1 LOGICAL AND PHYSICAL CONTROL AUDIT

Today's major concern for banks regarding to their IT system is how to guarantee the confidentiality and integrity of their various day to day processes and activities. Giving little consideration for IT logical and physical controls audit may create unauthorized data access and confidential information being retrieved by unauthorized users. Regarding to the respondents indicating in the below table 12, 37% of the respondents focused little extent attention for IT logical and physical controls audits, 28% of the respondents focused in moderate extent, 25% and 10% of the respondents gives great and very great extent for auditing IT logical and physical controls respectively. This indicates that, majority of the respondents' gives little attention for IT logical and physical control audit. The reason for giving little attention for IT logical and physical control audit were there are level of risk of occurrence of unauthorized network access was minimum.

Table 12 :- Practice of logical and physical control audit

Likert Scale	Frequency	Percent
Little extent	22	37%
Moderate Extent	17	28%
Great Extent	15	25%
Very Great Extent	6	10%
Total	60	1.0

Source: Questionnaire Results, 2020

4.3.1.2 IT ASSET MANAGEMENT AUDIT

Information Systems Audit and Control Association (ISACA, 2010), stated that, IT assets should be reviewed periodically in order to identify opportunities for enhancing efficiency, effectiveness and innovation in collaboration with service providers, service users and other stakeholders. And also the main objectives of reviewing bank's IT assets' is to determine whether adequate and effective IT asset management processes and controls are in place, in order to maintain the integrity of the IT assets (ISACA, 2010). Regarding to the respondents indicating in the below table 14, 1.7% of them have no extent at all in auditing IT asset management, 25% focused little extent attention for IT asset management audits. Yet the others 33.3%, 30% and 10% have moderate, great and very great attention for IT asset management audit respectively. Since the majority of the respondents highly focused on IT asset management audit. This implies that reviewing of IT assets management and services are important to ensure that the assets are deliver the greatest possible value in supporting the enterprise's strategy and objectives.

Table 13:- Practice of IT asset management audit

Likert Scale	Frequency	percentage
No Extent at all	1	1.7%
Little extent	15	25%
moderate Extent	20	33.3%
Great Extent	18	30%
Very Great Extent	6	10%
Total	60	100.0%

Source: Questionnaire Results, 2020

4.3.1.3 DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN AUDIT

(Dunkelberg, 2018), states that the internal IT auditor should periodically prepare an audit to fully evaluate and reinforce the effectiveness of the disaster recovery and business continuity plan for proper assurance. The primary objective of disaster recovery plan audit is to verify the merits of the plan and that it is adequate to ensure the timely resumption of business operations and processes during a disaster or other adverse conditions while reflecting the current operating environment of the business (Dunkelberg, 2018). According to the respondent's response indicating in the below table 14, 3.3% have no focus at all in auditing bank's disaster recovery and business continuity plan, 30% gives little attention, 40% gives moderate consideration on disaster recovery and business continuity plan audit, the rest 15% and 11.7% of the respondents gives great extent and very great extent in auditing disaster recovery and business continuity plan respectively. This indicates that majority of the respondents' gives great attention on reviewing the success of disaster recovery and business continuity plan of their banks.

Table 14:- Practice of Disaster recovery and business continuity plan audit

Likert Scale	Frequency	Percent
No Extent at all	2	3.3%
Little extent	18	30%
moderate Extent	24	40%
Great Extent	9	15%
Very Great Extent	7	11.7%
Total	60	100.0%

Source: Questionnaire Results, 2020

4.3.1.4 DATA BACKUP AND RESTORATION AUDIT

According to Control Objectives for Information and related Technology (COBIT, 2010), in order to restore corporate information, IT auditor must ensure and evaluate the safeguarding of data availability and integrity. As per the respondent's response observed in the below table 15, 3.3% of them have not focus on data backup and restoration audit, 26.7% of the respondents have little focus on data backup and restoration audit, 20% of the respondents have moderate focus on data backup and restoration audit and 31.7 % and 18.3% of the respondents gives great and very great focus on data backup and restoration audit. This indicates that majority of the respondents focused and conduct data backup and restoration audit in great level

Table 15:- Practice of Data backup and restoration audit

Likert Scale	Frequency	Percent
No Extent at all	2	3.3%
Little extent	16	26.7%
moderate Extent	12	20.0%
Great Extent	19	31.7%
Very Great Extent	11	18.3%
Total	60	100.0%

Source: Questionnaire Results, 2020

4.3.1.5 DATA PROTECTION AND PRIVACY AUDIT

Data protection and privacy is key main concern for banking sector. Not protecting and unlimited access of customers' data has been affects every level of banking activity and creates customer dissatisfaction, makes the failures of business. Workers at the banks need certain information to verify the identities of those accessing an account belonging to a client. Financial advisors require certain client data to enter into a transaction on the behalf of those holding an account with them. Employees in another area may also need this information for other functions within a bank or financial firm (Data Protection Laws of the World , 2019). As per the respondent's response observed in the below table 16, 73% of them have very great focus on data protection and privacy audit and the others 27% of the respondents have moderate focus on data protection and privacy audit. This indicates that majority of the respondents focused and conduct data protection and privacy audit in very great level.

Table 16:- Practice of data protection and privacy audit

Likert Scale	Frequency	Percent
Moderate Extent	16	27%
Very Great Extent	44	73%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.1.6 DATACENTER MANAGEMENT AUDIT

Data center is a core part for many organizations which can provide the place for all core devices, servers and storage and protect them to keep running properly and efficiently. These data centers have direct connection with business partners 'and must provide options for connectivity, power, cooling, backup, fire, water and smoking detection and multi-layered security to protect the integrity and high availability of data. Reviewing datacenter management is critical and mandatory for financial system (Worku, 2017). According to the respondent's response indicating the below table 17, 6.7% of the respondents gives little attention on datacenter management audit, 33.3% focused on moderate extent, 38.5% focused great extent and the rest 21.7% focused on very great extent. This indicates that majority of the respondents' gives great attention on datacenter management audit.

Table 17 :-Practice of datacenter management audit

Likert Scale	Frequency	Percent
Little extent	4	6.7%
Moderate Extent	20	33.3%
Great Extent	23	38.3%
Very Great Extent	13	21.7%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.1.7 SYSTEM AVAILABILITY AUDIT

Commercial banks in Ethiopia are established ATM, electronic fund transfer, online banking and others services supported by IT. Hence, System availability audit in the banking operation includes the availability of ATM service and online banking. Among the respondents indicating in the below table 18, 62% of the respondents have very great focus on system availability audit. Yet the others 38% of the respondents have great focus on system availability audit respectively. This indicates that majority of the respondents' gives very great attention on system availability audit.

Table 18 :- Practice of system availability audit

Likert Scale	Frequency	Percent
Great Extent	23	38%
Very Great Extent	37	62%
Total	60	1.0

Source: Questionnaire Results, 2020

4.3.2 CHALLENGES FACED IN CONDUCTING IT AUDT

The second objective of the study was to identify challenges faced during conducting IT audit assignments.

4.3.2.1 LACK OF AUDIT RESOURCES (TOOLS) USES DURING IT AUDIT

Resources refer to the availability of audit tools, time, budget and audit staff that the audit team could command to assist their IT auditing activities (Siew, et al, 2017). Siew et al. (2017) found that resource availability is one of the factors that challenges IT audit and according to the researchers this factor includes items like: whether computer-assisted auditing tools (CAATs) are used, whether there is enough time to conduct the IT audit, whether there is enough budget available to conduct the IT audit, and whether there is enough staff to properly conduct the IT audit (Siew, et al, 2017). According to the respondent's response indicating in the below table 19, 12% of them indicated that there is great extent of lack of audit tools uses during IT audit and the others 88% of the respondents indicated that there is very great extent of lack of audit tools to use during IT audit. This indicates that, majority of the respondents conduct IT audit assignment without IT audit tools. Lack of IT audit tools have very adverse effect on conducting IT audit.

Table 19: Lack of IT audit tools

Likert Scale	Frequency	Percent
Great Extent	7	12%
Very Great Extent	53	88%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.2.2 CHALLENGES OF COPING WITH TECHNOLOGY CHANGES

The rapid development and changes in the world of ICT require IT auditors to constantly updating their skills and technical knowledge. Also, very important for IT auditors are their competencies and skills and education in multi-disciplinary fields. Moreover, it is very important to the IT audit profession is to be certified in CIA, CISA, CISM or some other professional education (Komneni, 2008). According to the respondent's response stated in the below table 20, 11.3 % of them indicated that there is little challenges of coping with technology changes. The other 33.3% and 55% of the respondents respond that there is great and very grate challenges of coping with technology changes respectively. This implies that majority of the respondents have get challenges in coping of information technology changes due to the fact that they are not taken continuous professional certificates and continuous skill development rather they have only formal educational background.

Table 20:-Challenges in coping technology changes

Likert Scale	Frequency	Percent
Little extent	7	11.7%
Great Extent	20	33.3%
Very Great Extent	33	55%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.2.3 POOR ASSESSMENT OF THREAT AND VULNERABILITY

Properly planned and implemented threat and vulnerability management programs represent a key element in IT audit to detect threats and vulnerabilities and to provide mitigation strategy before happening business failures. As per the respondent's response indicated in below table 21, 10% of them indicated that there is little extent of poor assessment on threats and vulnerabilities. The other 42% and 48% of the respondents respond that there is great extent and very great extent of poor assessment on threats and vulnerabilities respectively. This implies that majority of the respondents have problems in assessing threats and vulnerabilities of IT audit assignments in very great extent.

Table 21:- Poor assessment of threats and vulnerabilities

Likert Scale	Frequency	Percent
Little extent	6	10%
Great Extent	25	42%
Very Great Extent	29	48%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.2.4 DIFFICULTIES ON THE IDENTIFICATION OF IT RISKS

The IIA's International Standards for the Professional Practice of Internal Auditing (Standards) specifically notes that internal auditors must assess and evaluate the risks and controls for information systems that operate within the organization. Internal auditors need to understand the range of controls available for mitigating IT risks. Identification of IT audit risk procedures are performed to obtain and understanding of organization and its environment, including organizations IT internal control, to identify and prioritize the risks. As per the respondent's response stated in below table 22, 15% of the respondents reflect that there is little extent of difficulties on the identification of IT risk while 26.7% reflect great extents and 58.3% respond that there is very great extent of difficulties on the identification of IT risk during conducting of IT audit assignment. This implies that majority of respondents have getting problems in identification of IT risks.

Table 22:- Difficulties on the identification of IT risks

Likert Scale	Frequency	Percent
Little extent	9	15%
Great Extent	16	26.7%
Very Great Extent	35	58.3%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.2.5 LACK OF MANAGEMENT APPRECIATION

Higher management support contributes better effects on IT auditor efficiency, it supports to get sufficient resources to do its function, and implemented recommendations. Among the respondents indicating in below table 23, 51.7% indicated that there is moderate extent on lack of management appreciation on the importance of IT audit. Yet the other 31.7% and 16.7% of the respondents indicated great extent and very great extent on lack of management appreciation of the importance of IT audit respectively. This indicates that, majority of the management lacks appreciation on the importance of IT audit.

Table 23:- Lack of management appreciation on the importance of IT audit

Likert Scale	Frequency	Percent
moderate Extent	31	51.7%
Great Extent	19	31.7%
Very Great Extent	10	16.7%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.2.6 LACK OF AUDITORS IT CONTROL KNOWLEDGE

The internal IT auditor's assurance is an independent and objective assessment that the IT-related controls are operating as intended. This assurance is based on understanding, examining, and assessing the key controls related to the risks they manage and performing sufficient testing to ensure the controls are designed appropriately and functioning effectively and continuously (Richard, 2005). IT internal auditors should have a capability to assess an organization's framework and internal audit practices for IT risk and control, compliance, and assurance. Regarding lack of IT control knowledge gap by IT auditor presented in the below table 24, 6.7% of the respondents indicated that there is moderate extent on lack of IT control knowledge by IT auditors and the other 33.3% and 60% of the respondents respond that there is great extent and very great extent on lack of IT control knowledge by IT auditors respectively. This indicates that, majority of the IT auditors lacks IT control knowledge.

Table 24:- IT control knowledge gap by IT auditor

Likert scale	Frequency	Percent
moderate Extent	4	6.7%
Great Extent	20	33.3%
Very Great Extent	36	60%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.3 IT RELATED FRAUDS

Analysis of respondents' responses showed that, commercial banks in Ethiopia have encounter different types of IT related frauds which are listed and described below.

4.3.3.1 UNAUTHORIZED NETWORK ACCESS

Quick information accessibility on the internet has become increasingly important for growing banking businesses. Banking industries are beginning to spread various business functions to the public network, securities are highly needed to make sure that their network not been tampered with or does not fall to wrong hands. If a network is accessed by a hacker or dissatisfied employee, it could create disaster for organization branded data, affect company productivity negatively, and hinder the ability to compete with other businesses. Unauthorized network access can also harm a company's relationship with customers and business partners who may question the company's ability to protect their confidential information. Among the respondents' response indicated in the below table 25, 71.7% of the responses have no extent at all to access unauthorized network, 18.3% responses have little extent in accessing unauthorized network and the rest 6.7% there is moderate extent in accessing unauthorized network, this implies that there is little extent of occurrence of IT related frauds by retrieving unauthorized network access.

Table 25:- Unauthorized network access

Likert scale	Frequency	Percent
No Extent at all	43	71.7%
little extent	11	18.3%
moderate Extent	4	6.7%
Great Extent	2	3.3%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.3.2 SNIFFING

Banking applications belong to the most security critical and data sensitive application category. Cashless mobile payment has significantly fragmented the traditional financial services, beginning with the first ATM and ending in e-banking. Users often misconceive that banking applications provide secure transactions and an easy-to-use interface, by assuming all communications are done between local banking applications and remote bank servers securely. However, sniffing is a common network security attack in which a program or device takes important information from the network traffic of specific network. Various protocols are also disposed to sniffing. Sniffing is an attack on confidentiality of data. The basic target of sniffer is to find out the password and other personal information of the user, this compromise the confidentiality. Regarding to the responses about sniffing indicating in the below table 26, 70% of the respondents reflect that there is no extent at all on sniffing while the other 23.3% and 6.7% of the respondents reflect that there is little extent and moderate extent towards sniffing respectively. This implies that, there is little extent at all in the occurrence of being able to seeing plain text login credentials and confidential information (sniffing).

Table 26 :-Sniffing

Likert scale	Frequency	Percent
No extent at all	42	70.0%
Little extent	14	23.3%
moderate Extent	4	6.7%
Total	60	100.0

Source: Questionnaire Results, 2020

4.3.3.3 HACKING

Malicious hacking is becoming prevalent in the banking sector with the increasing popularity of the internet, e-Baking and e-Commerce. Here, the primary motive of malicious or unethical hacking involves financial gain or stealing valuable information. Regarding to respondents’ responses indicating in the below table 27, 76.7% of the respondents reflect that there is little extent on hacking while the other 16.7% and 6.7% of the respondents reflect that there is moderate extent and very great extent of hacking. This implies that there is moderate extent of accessing a computer network by circumventing its security system.

Table 27:- Hacking

Likert scale	Frequency	Percent
little extent	46	76.7%
moderate Extent	10	16.7%
Very Great Extent	4	6.7%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.3.4 DATA INTERCEPTION DURING FILE UPLOAD

Data validation is a crucial tool for every business as it ensures your team can completely trust the data they use to be accurate, clean and helpful at all times. Making sure the upload data is correct is a proactive way to safeguard company's most valuable, demand-generating assets. Usage of data validation during uploading of customer file is important. Because incorrect bank data is a major source of customer frustration, waste of time and resource. Data interception during file upload includes, incorrect phone number, fake name, incorrect e-mail address and incorrect account number.

Among the respondents' response indicating below table 28, 35% of them indicated that there is great extent of fraud on data interception during file upload and the other 65% of the respondents indicated that there is very great extent of fraud on data interception during file upload. This implies that there is very great extent of fraud on data interception during file upload.

Table 28:-Data interception during file upload

Likert scale	Frequency	Percent
Great Extent	21	35%
Very Great Extent	39	65%
Total	60	100%

4.3.3.5 INSIDER THREAT

The threats that insiders pose to government organizations, businesses, and institutions continue to be a critical concern. Because insiders have access to valuable information assets that are unavailable to outsiders, damages resulting from insider attacks can be devastating. Furthermore, these threats are increasing in scale, scope, and sophistication; thus, emphasizing the critical need for organizations to apply current security techniques. The major common types of insider threats are, modification or stealing of confidential or sensitive information for personal use, theft of customer information to be used for business advantage and interruption of an organization data, system or network (Secure & Barrios, 2016). Among the respondents' response stated in below table 29, 11.7% of them indicated that there is little extent of fraud on insider threat and the other 75% of the respondents indicated that there is great extent of fraud on insider threat. However, 13.3% of the respondents indicated that there is very great extent of fraud on insider threat.

Table 29; - Insider threat

Likert scale	Frequency	Percent
Little extent	7	11.7%
Great Extent	45	75.0%
Very Great Extent	8	13.3%
Total	60	100.0%

Source: Questionnaire Results, 2020

4.3.3.6 PHISHING

The phishing attack has become one of the most common financial crimes in recent years. Phishing is defined as "a criminal activity using social engineering techniques that enables phishers to attempt fraudulently acquire sensitive information, such as passwords, credit card details, passport card information etc., by masquerading as a trustworthy person or business in an electronic communication (Hall, 2011).

Among the respondents' response indicating in the below table 30, 38.3% of them indicated that there is little extent of fraud on phishing and the other 33.3% of the respondents indicated that there is moderate of fraud on phishing. However, 28.3% of the respondents indicated that there is great extent of fraud on phishing. This implies that, extent of phishing is very great extent.

Table 30:- Phishing

Likert scale	Frequency	Percent
Little extent	23	38.3%
moderate Extent	20	33.3%
Great Extent	17	28.3%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.3.7 MALWARE PROGRAMS

Hackers use the malicious programs to gain control of targeted computer in order to use it further for other types of cyber-attacks. As a result, malicious software has turned into big business and cyber criminals became profitable organizations and able to perform any type of attack. An understanding of today’s cyber threats is a vital part for safe computing and ability to respond the cyber attackers (Wajeb G and Abdulrahman M, 2011).

Among the respondents’ response indicating in the below table 31, 11.67% of them indicated that there is little extent of fraud on malware program and the other 18.33% of the respondents indicated that there is moderate of fraud on malware program. However, 23.33% and 46.67% of the respondents indicated that there is great extent and very great extent of fraud on malicious programs. This implies that, extent of malicious program is very great extent.

Table 31:- Malware program

Likert scale	**Frequency**	**Percent**
Little extent	7	11.67%
moderate Extent	11	18.33%
Great Extent	14	23.33%
Very Great Extent	28	46.67%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.4 IT AUDIT AND FRAUD DETECTION APPROACHES

The following section provides IT audit fraud detection approached implemented against IT related frauds.

4.3.4.1 NETWORK SECURITY ANALYSIS

Network security analysis involves the close inspection of a network's structure, data, and traffic in order to observe, detect, and eliminate potential vulnerabilities, threats and detect and prevent IT related frauds. Hence to perform network security testing and analysis, IT auditor needs audit tools. As per the respondent’s response indicating in below table 32, 25% and 30% of the respondents indicated that there is no extent at all and little extent of network security analysis respectively and the other 26.7% and 18.3% of the respondents indicated that there is moderate extent and great extent of network surveying. This implies that, majority of the respondents have little extent on network security analysis to detect IT related frauds.

Table 32:- Network security analysis

Likert scale	Frequency	Percent
No Extent at all	15	25%
Little extent	18	30%
moderate Extent	16	26.7%
Great Extent	11	18.3%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.4.2 PORT SCANNING

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities. As per the respondent’s response representing in below table 33, 10% of them indicated that there is very great extent of port scanning and the other 18% and 72% of the respondents indicated that there is little extent and no extent at all on port scanning. This indicates that, majority of the respondents’ performing port scanning in little extent to detect IT related frauds.

Table 33:- Port scanning

Likert scale	Frequency	Percent
No Extent at all	43	72%
Little extent	11	18%
Very Great Extent	6	10%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.4.3 VULNERABILITY SCANNING

Banking industry is an attractive target for criminals and other malicious actors. Because majority of banking operation is highly dependent on e-banking, mobile payments. Hence vulnerability assessment is determining whether the bank's network vulnerabilities can be exploited, in terms of confidentiality, integrity and availability and mitigation recommendations in order of priority. As per the respondent's response presented in the below table 34, 20% and 31.7% of the respondents indicated that there is little extent and moderate extent of vulnerability scanning respectively and the other 28.3% and 20% of the respondents indicated that there is great extent and very great extent on vulnerability scanning. This implies that, majority of the respondents perform vulnerability scanning in moderate extent.

Table 34:- Vulnerability scanning

Likert scale	Frequency	Percent
Little extent	12	20%
moderate Extent	19	31.7%
Great Extent	17	28.3%
Very Great Extent	12	20%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.4.4 PHYSICAL SECURITY CHECKS ON IT ASSETS

All the authorized staffs who access information asset room need to be physically verified and must carry an identity card, if possible implement digital access control or any biometric access control. As per the respondent's response indicating in the below table 35, 13% of them indicated that there is moderate extent of physical security checks on IT assets and the other 66.7% and 20% of the respondents indicated that there is great extent and very great extent of physical security checks on IT assets. This implies that, majority of the respondents check physical security of IT assets in great level in order to prevent and detect IT related frauds.

Table 35:- Physical security check on IT assets

Likert scale	Frequency	Percent
moderate Extent	8	13.3%
Great Extent	40	66.7%
Very Great Extent	12	20.0%
Total	60	100%

Source: Questionnaire Results, 2020

4.3.4.5 USES OF DATA ANALYSIS

Data analysis enables IT auditors to analyze an organization's business data to gain insight into how well internal controls are operating and to identify transactions that indicate fraudulent activity or the heightened risk of fraud. Data analysis also provides an effective way to be more proactive in the fight against fraud. Calculation of statistical parameters, stratification of numbers, joining of different diverse sources, duplication test and validation of entry dates are some of data techniques. Among the respondents indicated in the below table 36, 82% of them respond that there is very great extent of use of data analytics while the other 18% of them respond that there is moderate extent of use of data analytics. This indicated that, majority of the respondents' uses data analysis in order to detect IT related frauds.

Table 36:- Data analysis

Likert scale	Frequency	Percent
moderate Extent	11	18%
Very Great Extent	49	82%
Total	60	100.0

Source: Questionnaire Results, 2020

CHAPTER FIVE

5. SUMMARY, CONCLUSIONS AND RECOMMENDATION

This chapter presents conclusions drawn from the study, recommendations based on the evidences presented during the course of the study and as well as suggestions for future research. The subsequent discussion presents conclusions, recommendations and direction future research in an orderly manner.

5.1 SUMMARY OF THE STUDY

IT has become pervasive and critical in successful operations and management of any organizations especially financial institutions like banks. It is necessary to perform IT audits in companies due to the fact that information system integrity protection has become an important business issue in today’s business conditions, when companies’ core activities are becoming more tightly linked with their information systems. Thus, it has become necessary to audit the information systems of organizations. IT audits are important organizational processes that add value to the organization because they have given an assurance on the integrity, reliability and quality of the information produced by the organization’s information systems. IT audit in Ethiopia is at infant stage and it has given focus in recent years. The general objective of this research is to assess the practice of information technology audit in fraud detection in commercial banks of Ethiopia. In summary, by way of responding the research objectives, the study has been able to assess the level of IT audit focus area, identify challenges in conducting IT audit, assess the level of IT related frauds, evaluate the level of IT audit detection approaches against IT related frauds.

The present study successfully delivered all answers of the research questions. Based on the analysis and the findings, the following conclusions are drawn from the study:

As per the first objective, the result of the study indicated that, majority of the respondents gives little attention for auditing IT logical and physical controls. IT asset management audit were highly focused by majority of the respondents. Disaster recovery and business continuity plan review were gives great level of responses. Majority of the respondents were focused and conduct data protection and privacy audit, data backup and restoration audit and system availability audit in very great level. Conducting datacenter management audit gives great attention by majority of the respondents.

As per the second objective, the result of the study indicated that, majority of the respondents had luck of IT audit tools during conducting IT audit assignment. Majority of the respondents have get challenges in coping of information technology changes. Majority of the respondents have problems in assessing threats and vulnerabilities during conducting IT audit in very great extent. Majorities of the respondents gets problems in very great level during identification of IT risks. Majority of the respondents had get challenges due to lack of management appreciation for IT audit importance and lack of IT auditors' IT control knowledge in very great level.

As per the third objective, the result of the study indicated that, there is little extent on the occurrence of unauthorized network assess and occurrence of being able to seeing plain text login credentials and confidential information (sniffing). There is moderate extent of accessing a computer network by circumventing its security system (hacking). Majority of the respondents agreed that there is very grate level of data interception during file uploading. There is great extent on the occurrence of insider threats. Majority of the respondents agreed that occurrence of phishing and malware programs are very great extent.

As per the fourth objective, the result of the study indicated that, majority of IT auditors' uses network surveying approach in moderate extent, scanning of port to detect and prevent IT related frauds in little extent. Assessing vulnerability scanning could be performed in moderate level, whereas physical checking of IT assets could be conducted in great level.

5.2 CONCLUSION

The concept of IT auditing is practiced permanently with great variations among the banks and focuses were given to each of the areas of availability, confidentiality and integrity. For example, IT logical and physical access control audit, IT asset management audit, Disaster recovery and business continuity plan audit, database management audit, data backup and restoration audit, system availability audit and data protection and privacy audit are the listed one that are conducted by commercial banks of Ethiopia in different rates. In addition to this, the field of IT auditing and assurance is still relatively new and an emerging phenomenon in Ethiopia, challenges commonly faced during conducting of IT audit were lack of audit tools, challenges in coping information technology changes, identification of IT risk, lack of appreciation by the management on the importance of IT audit and lack of IT auditors' knowledge on IT controls. Most common IT related frauds existed in commercial banks of Ethiopia are, unauthorized network access, sniffing, phishing, malware programs, insider threats and data interception during uploading of files. The study recognized that the common IT audit approaches used to detect IT related frauds were include network surveying, port scanning, vulnerability scanning and checking the presence of IT assets.

5.3 RECOMMENDATION

Based on the findings the researcher makes the following recommendation: -

- All of the commercial bank’s found in Ethiopia, operations and functions are computerized and there need to be practice of IT auditing. However, from the study findings, the extent and focus given to IT audit areas is moderate. Therefore, the study suggested that the practice of conducting IT audit assignment improved by considering confidentiality, availability and integrity.

- As implied in the summary parts, there are challenges in conducting IT audit. Hence, to reduce such challenges, the study suggested that, top-level management communicate regularly IT auditors and follow up the implementation of IT audit findings

- The study also suggested that, IT auditors update their knowledge and skill continuously by taking different IT audit certification in order to cope up technology changes.

- Providing the whole necessary audit resources (audit tools) for the IT audit staff in order to conduct IT audit and detect IT related frauds effectively and efficiently.

- The study also proposed that, in order to detect IT related frauds, IT auditors’ focus in planning and identification of IT related risks in order to identify potential risk areas and events that banking sectors needs to mitigate fraud.
- The study recommended that, regular evaluation of IT control is important in order to determine their effectiveness in detecting fraud and identify weaknesses.

5.4 SUGGESTIONS FOR FURTHER STUDY

This study concentrated only on the banking sector; hence, future studies will be carried out among other financial institutions i.e. insurance companies and microfinances.

REFERENCES

Abdallah, A. (2016). Fraud detection system: A survey. *information Assurance and Security Research Group, Vol 68*, 90–113. Retrieved June 2016, from https://doi.org/10.1016/j.jnca

Aeran, A. (2010). *Comprehensive overview of Insider Threats and their controls.* School of Business. Austria : Bond University .

Albrecht, W. (2010). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia - Social and Behavioral Sciences*, 97-102. doi:10.1016/j.sbspro

Alemayehu, E. (2016). *The role of internal audit in detecting fraud: the case of Ethiopian budgetary public sectors.* College of Bussiness and Economics. Addis Ababa: Addis Ababa University.

Alraja & Lomiam. (2013). The Effect of General Controls of Information System Auditing in the Performance of Information Systems. *Interdisciplinary Journal of Contemporary Research in Business, Vol 5*.

Anchugam & Thangadurai. (2018). Introduction to Network Securit. In *Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications* (pp. 33-80). Retrieved from http://doi:10.4018/978-1-5225-3923-0.ch003

Axelsen, et al. (2011). Examining the Role of IS Auditing in the Public Sector. *The Pacific Asia Conference on Information Systems (PACIS).* AIS Electronic Library (AISeL. Retrieved from http://aisel.aisnet.org/pacis2011/23

Barrios, R. M. (2016). A multi-leveled approach to intrusion detection and the insider threat. *Journal of Information Security, Vol 4*(1), 56-64. doi:10.4236/jis.2013.41007.

Bellino, M. (2010). *Global Technology Audit Guide (GTAG) 8 Auditing Application Controls.* Florida: The IIA Research Foundation.

Belloli. (2006). The Auditor's Responsibility to Consider Fraud in an Audit of a Financial Report. *Auditing and Assurance Standards Board (AUASB). Vol 3*, pp. 91-95. Melbourne: AUASB.

Bhasin, M. L. (2015). An emprical study of frauds in the banks. *European Journal of Business and Social Sciences, 4*, 1-12. Retrieved from http://www.ejbss.com/recent.aspx-/

Björklund, J. and Joelsson, R. (2015). *A New Approach for IT Audit: Testing the Theory of Technology Debt in an IT Audit Setting.* University of Guthenberg, School of Business, Economics and Law.

Bzuwerk, Y. (2018). *Factors affecting the quality of information technology audit in Ethiopian commercial banks.* MSC Thesis , Addis Ababa University , Accounting and Finance, Addis Ababa.

Chakrabarty, W. (2013, August). Fraud in the banking sector- causes, concerns and cures. *RBI Monthly Bulletin*, pp. 95-106.

Champlain, J. J. (2012). *Auditing Information Systems, IT Audit Handbook* (2, ed.). John Wiley & Sons.

Coderre D.G. (2010). *Fraud Analysis Techniques using ACL.* John Wiley & Sons.

Collins, L. (2013). *Computer and Information Security Handbook.* (Third, Ed.)

Creswell, J. (2014). *ResearchDesign Qualitative, Quantitative, and Mixed Methods Approaches.* (4e, Ed.) SAGE Publications. Inc.

Daniela, A. (2014, May 16-17). The Role of Internal Audit in Fraud Prevention and Detection. *Procedia Economics and Finance*, 489 – 497. doi:10.1016/S2212-5671(14)00829-6

Data Protection Laws of the World . (2019). Retrieved from DLA Piper: https://www.dlapiperdataprotection. com/index.html?t=law&c=MX&c2=

Dunkelberg, D. (2018). *The role of IT audit in disaster recovery plan.* Gaza: I.S Partneres LLC.

Goldmann, P. (2009). An Introduction to Cyber Fraud. In *Anti-Fraud Risk and Control Workbook* (pp. 149-161).

Hall, J. A. (2011). *Information Technology Auditing and Assurance* (3, illustrated ed.). South-Western: South-Western Cengage Learning.

Harb, R. (2012). *The Impact of Information Systems Audit on Improving Bank's Performance:.* MSC Thesis , Applied Study at Banks Working in Gaza.

ISACA. (2010). *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals.*

James A.Hall. (2011). *Information Technology Auditing and Assurance* (Vol. 6e). Lehigh University.

Jonathan Adegoke1, K. S. (2013). Effectiveness of Internal Auditor in Controlling Fraud and Other. *Research Journal of Finance and Accounting*.

Julia, M. (2013). *Information Technology Audit and Fraud prevention in commercial banks of Kenya.*

Komneni, V. (2008). *ICT Auditing and Required Competencies.*

Kothari, C. (2004). *Research Mathodology : Methods and Techniques* . EBX-publisher .

Kozlovs, D. et al. (2015). *Towards Continuous Information Security Audit.* Riga Technical University, Latvia.

Kumar, R. (2011). *Introduction to Research Methodology.*

Launius S.M. (2010). *Securing the Network Perimeter of a Community Bank.* SANS Institute.

Lee & Kerlinger. (2011). *Foundations of Behavioral Research.*

Lovaas & Wagner. (2012). IT Audit Challenges for Small and Medium- Sized Financial. *Annual Symposium on Information Assurance & Secure Knowledge Management.* Albany, ny.

Lovaas, P. (2012). *A Comprehensive Risk-Based Auditing Framework for Small- and MediumSized Financial Institutions.* Issues in Information Systems, Dakota State University.

Mengistu, B. (2016). *Auditing IT and IT Governance in Ethiopia, Addis Ababa University.*

Merhout, J., and Havelka, D. (2010). "Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit'. *Comm Assoc InfoSyst*, 463-483.

Mulwa D. (2012). *Survey of Insider Information Security Threats Management in.*

Ndulu, E. (2004). *A survey of the causes of IS failure among microfinance institutions in kenva.* University of Nairobi.

Nkwe, N. (2011). State of Information Technology Auditing in Botswana. *Asian Journal of Finance*.

Nkwe, N. (2011). State of Information Technology Auditing in Botswana. *3*.

Norman, G. (2003). *Health Measurement Scales: A practical guide to their development and use.* Oxford University Press.

Nzuki, C. (2006). *A survey of ICT Audit in commercial banks of Kenya.* Faculty of Business Administration . Kenya: University of Kenya.

OFAG. (2017). *The Office of Federal Auditor of Ethiopia IT Audit Mannual.*

Olatunji, O. (2014). *Impact of internal control system in banking sector in Nigeria.*

Panwar,et al. (2014). *WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.*

Patrick, D. (2011). *Managing Information Security Risk: Organization, Mission, and Information U.S. Special Publication 800-39.*

Rahel, A. (2016). *Capital Investment Decisions on Information Technology and Its Impact on the.* Department of Accounting and Finance. Addis Ababa: Addis Ababa Univrsity.

Rahman, A. e. (2014, September 2014). Sustainability in Information Systems Auditing. *Vol 3*.

RBI. (2011). *Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds.*

Richard et al. (2010). *GTAG- Global Technology Audit Guide, Information Technology Controls,*. The Institute of Internal Auditors.

Rotim & Komnenić,. (2010). *Improvement of Business and IT Alignment through IT Internal Audit.*

Rouse, M. (2016, September). Retrieved from TechTarget.com.

Sandra Senft, Frederick Gallegos, and Aleksandra Davis. (2012). Information Technology Control and Audit ISBN 9781439893203 Auerbach Publications.

Secure, J., & Barrios, R. (2016). A multi-leveled approach to intrusion detection and the insider threat. 56-64.

Siew, et al. (2017). *Factors affecting IT Audit Quality: an Exploratory Study*. Monash University Malaysia, School of business. Malasia: Bandar Sunway.

Singh. N.P. (2010). Online Frauds in Banks with Phishing. *Journal of Internet banking and commerce*.

Singleton, T. (2014). The Core of IT Auditing. *ISACA Journal Volume 6*.

Stoel, et al. (2012). *An Analysis of Attributes that Impact Information Technology Audit* (Vol. 13).

Tariku, D. (2018). *Assessment of Information System Audit Effectiveness a case of Commercial Bank of Ethiopia*. Addis Ababa: St' Marry University.

Veerankutty & Mahzan. (2010). IT Auditing Activities of Public Sector Auditors in Malaysia. *African Journal of Business Management*, *Vol 5*, 1551-1563.

Wagner, J. (2011). *Information System Auditing and Electronic commerce.*

Wajeb G and Abdulrahman M. (2011). Software Vulnerabilities, Banking Threats, Botnets and Malware Self-Protection Technologies. *IJCSI International Journal of Computer Science Issues*, 236-241. Retrieved from http://www.ijcsi.org/

Walker, J. (2015). *Continuous IT System Auditing.*

White, S. K. (2019). IT asset management (ITAM): A centralized approach to managing IT systems and assets.

Wikipedia. (2012). *Advance Fee Fraud*. Retrieved from the free encyclopedia : http://www.wikipedia.org/wiki/advancefeefraud

William, B. et al. (2013). IT Auditing and Application Controls for Small and Mid-Sized Enterprises. *Revenue, Expenditure, Inventory, Payroll, and More*.

Wonde. (2014). Retrieved from Data Protection Policy: https://www.wonde.com/data-protection-policy

Worku, G. (2017). *Data Center Virtualization framework In Banking Sector: THE CASE OF WEGAGEN BANK S.C.* Department of Information technology . Addis Ababa: Addis Ababa University.

Zikmund, W. G. (2003). *Business Research Methods.* Indian: Thomson/South-Western.

APPENDIX

St. Mary's University

College of Graduate Studies

MBA in Accounting and finance

Dear participant,

This study is about the "**Assessing Practice of Information Technology Audit and Fraud Detection on Commercial Banks in Ethiopia**" as a requirement in the completion of Master's Degree in Accounting and Finance.

Enclosed are survey questions to be filled out to the best of your knowledge and professional integrity. The information will be used for the academic purpose. Your volunteer participation is appreciated and the information you provide will have an added value for the research, as well it will be kept confidential. Returning the completed survey on time will again be appreciated.

If you have any clarification, please don't hesitate to contact me at tgalex7@gmail.com .

Thank you

PART 1:- PARTICIPANT INFORMATION

Please provide your background information by ticking the most appropriate box in each of the following questions.

1. Gender Male □ Female □
2. Age 25-35 □ 36-46 □ above 46 □
3. Level of Education Degree □ Master's □ above □
4. How long have you been working in the bank?
   Less than 2 years □ 2-5 years □
   6-10 years □ more than 10 years □
5. What is your overall experience in IT/IS auditing?
   Less than 5 years □ 5 to 10 years □ More than 10 years □

6. What is your highest level of professional certification?

Certified Information Systems Audit □

Certified Public Accountant □

Microsoft Certified Systems Auditor □

No professional certification □

Others [Specify]________________________

PART 2: IT AUDIT AND FRAUD DETECTION

1. Who conduct IT audit in your bank?

Internal Audit Department staffs □

External IT consultant □

Audit firms □

Others [specify] ____________________________________

2. Where do the IT auditors of the bank refer auditing guidelines for IT audit assignment?

Bank's Internal Audit guideline □

Government organization audit guideline □

International auditing guideline □

Others [specify] ____________________________________

3. How often does the bank conduct IT audit assignment?

Once a year □

Twice a year □

Continuous □

Never □

Others [specify] ____________________________________

4. What reports are provided after conducting IT audit in the bank?

Technical report □

Management report □

Both technical and management report □

5. To whom does the IT audit team report?

Board Audit Committee □

Board Information and Technology Committee □

Chief Executive Officer (CEO) □

Chief Information Technology Officer (CITO) □

Chief Internal Audit Officer (CIAO) □

Others [specify] ____________________________________

6. The following are referring to possible IT Audit focus areas in the bank. Please indicate your professional view and agreement on the extent of IT audit focus area in your bank in terms of the following points by ticking "✓" the scale.

	No Extent At All	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
IT Audit Focus Areas	**1**	**2**	**3**	**4**	**5**
Logical and physical control					
IT asset management					
Disaster recovery and business continuity plan					
Data backup and restoration					
Data protection and privacy					
Datacenter management					
System availability					
Other (specify and rate accordingly)					

7. The followings are possible challenges faced in conducting IT auditing. Please indicate your professional view and agreement on the extent of the challenges faced in conducting IT auditing in your bank in terms of the following points by ticking "✓" the scale.

	No Extent At All	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
Challenges faced in conducting IT Audit	1	2	3	4	5
Lack of Audit tools to use during IT Audit					
Challenges of coping with technology changes					
Poor assessment of threats and vulnerabilities.					
Difficulties on the identification of IT risk					
Lack of management appreciation of the importance of IT audit					
Lack of IT auditor IT control knowledge					
Others [specify and rate accordingly]					

8. The followings are IT related frauds occurred in the banks. Please indicate your professional view and agreement on the extent to which the bank has encountered each of the following IT related frauds by ticking "✓" the scale.

IT related frauds	**No Extent At All**	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
	1	2	3	4	5
Unauthorized network access					
Sniffing					
Hacking					
Data interception during file upload					
Insider threats					
Phishing					
Malware code					
Others [specify and rate accordingly]					

9. The followings are detection approaches for IT related frauds in the banks. Please indicate your professional view and agreement on the extent to which you use each of the following approaches in detecting and preventing IT related frauds in the bank by ticking "✓" the scale.

Detection and prevention approaches	**No Extent At All**	**Little Extent**	**Moderate Extent**	**Great Extent**	**Very Great Extent**
	1	2	3	4	5
Network surveying					
Port scanning					
Vulnerability scanning					
Physical security checks on IT assets					
Use of data analytics					
Others [specify and rate accordingly]					