ST. MARY'S UNIVERSITY
SCHOOL OF GRADUATE STUDIES

INFORMATION TECHNOLOGY AUDITING PRACTICE: A CASE STUDY OF SELECTED PRIVATE COMMERCIAL BANKS IN ETHIOPIA

BY LULA AWOL

MARCH 2023
ADDIS ABABA, ETHIOPIA

INFORMATION TECHNOLOGY AUDITING PRACTICE: A CASE STUDY OF SELECTED PRIVATE COMMERCIAL BANKS IN ETHIOPIA

BY

LULA AWOL YIMAM

ADVISOR: MESERET MINLARGEH (PHD)

A THESIS SUBMITTED TO ST. MARY UNIVERSITY, SCHOOL OF GRADUATE STUDIES, IN PARTIAL FULFILMATION OF THE REQUIREMENT FOR THE DEGREE OF MASTERS OF BUSINESS ADMINSTRATION IN ACCOUNTING AND FINANCE

March, 2023
ADDIS ABABA, ETHIOPIA

INFORMATION TECHNOLOGY AUDITING PRACTICE:

A CASE STUDY OF SELECTED PRIVATE COMMERCIAL BANKS IN ETHIOPIA

BY

LULA AWOL YIMAM

ID No. SGS/0213/2013A

Approved By Board of Examiners

Dean, Graduate Studies ______________

Signature

Advisor ______________

Meseret Milargeh (PHD) **Signature**

External Examiner ______________

Demis H/Gebriel (PHD) **Signature**

Internal Examiner ______________

Mohammed Seid (PHD) **Signature**

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: Lula Awol

Signature: _____________

Date: March, 2023

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

Name: Meseret Milargeh (PHD)

Signature: __________________

Date: March, 2023

Acknowledgments

Writing this thesis has been an amazing journey, and I'd like to thank everyone who has helped me along the way. First and foremost, I would like to express my gratitude to the Almighty God and his virgin mother, Saint Mary, for their invaluable assistance in completing this research project and for their unwavering support in the success of my entire life.

I'd like to thank Dr. Meseret Milargeh, my thesis advisor, for his unwavering support and guidance throughout my research and writing process. He gave me invaluable advice and feedback, and his vast knowledge aided in the development of my project.

I'd also like to thank my family for their encouragement and love. They have been an incredible source of support and have kept me motivated throughout the duration of my project.

I'd also like to thank my friends and colleagues, whose perspectives and insights have been invaluable. They have aided in the development of my project and contributed to a better understanding of the subject.

Finally, I'd like to thank everyone who has contributed to the success of this project. Their hard work and dedication have been instrumental in assisting me in reaching my objectives. Thank you all for your help and support. It has been a pleasure to collaborate with you all.

Abstract

The main purpose of this study was to assess the challenges of an information technology audit in the case of 16 sampled private commercial banks. A purposive sampling method was used, and data were collected using structured questionnaires. A descriptive type of research design was used, and data were collected from all IT audit employees that are working in the internal audit department of each bank. A total of 41 questionnaires were distributed to the information technology auditors of all private commercial banks, and 41 (100% response rate) were collected. The data were run with SPSS version 22, and mean analyses were carried out to assess the challenges of an information technology audit. communication barrier with the IT department; a failure to attend regular audit committee meetings; no long-term strategy to transform IT audit into a data-driven function; a failure to engage in technological projects; a shortage of skilled manpower to conduct IT audits; and security and privacy challenges. These are among the challenges identified in this study. This highlights the importance of IT audits adopting a next-generation mindset and implementing the governance, methodologies, and enabling technologies required to support today's highly dynamic and fast-moving banks. An effective IT audit framework must be able to detect these changes in order to protect the organization from potential threats. An IT audit must be able to access and govern the data being used in order to ensure that various control and compliance requirements are met. The ability to leverage advanced technologies in IT auditing, in particular, is highly dependent on the quality of the data in the bank.

***Keywords**: Information Technology Audit; Information Technology Audit challenge; commercial banks*

Table of contents

List of Tables

Acronyms

GOE-Government of Ethiopia

BoD – Board of Directors

CAE – Chief Audit Executive

CBE-Commercial Bank of Ethiopia

CEO – Chief Executive Officer

DBE -Development Bank of Ethiopia

IA – Internal Audit

IAD – Internal Audit Department

IAF – Internal Audit Function

IIA – Institute of Internal Auditor

IPPF – International Professional Practice Framework

IT-Information Technology

NBE- National Bank of Ethiopia

RTGS-Real Time Gross Settlement

CIA- Certified Internal Auditor

CISA- Certified Information Systems Auditor

CISSP - Certified Information Systems Security Professional

CRISC - Certified in Risk and Information Systems Control

Chapter One

I. Introduction

1.1. Background of the Study

Today's banking environment is extremely competitive. To be able to survive and grow in a changing market environment, banks are turning to the latest technologies, which are viewed as a "enabling resource" that can aid in the development of learner and more flexible structures that can respond quickly to the dynamics of a rapidly changing market scenario. It is also regarded as a tool for cost reduction and effective communication with people and institutions involved in the banking industry(Chauhan & Sheetlani, 2019).

Information technology enables sophisticated product development, improved market infrastructure, the implementation of dependable risk-control techniques, and the ability of financial intermediaries to reach geographically distant and diverse markets. The internet has had a significant impact on bank delivery channels. The internet has emerged as a vital medium for the delivery of banking products and services (Sarens et al., 2012).

Although the GOE permitted the establishment of commercial banks and insurance companies in 1994, foreign ownership in this sector is still prohibited. Ethiopia's banking sector currently consists of a central bank (The National Bank of Ethiopia, or NBE), one state-owned development bank, one government-owned commercial bank, and nineteen commercial banks. In terms of assets, deposits, bank branches, and total banking workforce, the state-owned Commercial Bank of Ethiopia (CBE) dominates the market. The Development Bank of Ethiopia (DBE) is another government-owned bank that lends to stockholders in priority sectors. The NBE aims to promote monetary stability and a sound financial system by maintaining credit and exchange conditions conducive to the economy's balanced growth. In 2015, the NBE authorized commercial banks to offer mobile banking and agent banking. Many commercial banks expanded their service offerings to include mobile and agent banking as a result of the NBE's perm (*Privacy Shield*, 2019).

IT is transitioning from a back-office function to a primary aid in increasing a bank's value over time. IT accomplishes this by maximizing banks' proactive measures such as strengthening and standardizing banks' infrastructure in terms of security, communication, and networking, achieving inter-branch connectivity, transitioning to a Real Time Gross Settlement (RTGS) environment, forecasting liquidity by building real-time databases, and using Magnetic Ink Character Recognition and Imaging technology for cheque clearing, to name a few.

The increased reliance on IT and the complex, evolving nature of IT systems, has resulted in the need to implement internal controls to safeguard commercial information(Stoel & Muhanna, 2011). The management of IT risks has to be a key part of corporate governance; therefore, the effective and efficient management of IT is vital to the success of most organizations(Members, 2003). The dependability of computerized data and the systems that process, maintain, and report these data, as well as the protection of the organization's assets and data, and ensuring efficient operations, are all major concerns and functions of information technology (IT) audit (Siew E. e., 2017; Singleton, 2014).

Information technology (IT) audits are responsible for guaranteeing the reliability of computerized data and the systems that handle, maintain, and report it, as well as preserving the organization's assets and data and maintaining efficient operations. Banks and other financial institutions must design an information technology audit program to support their information technology infrastructure, keep non-public client information secure, and undertake a risk-based audit, according to rule(Cole, 2014).

The study assessed the practice of IT audit work in order to achieve successful IT auditing in the case of selected commercial banks in Ethiopia.

1.2. Statement of the Problem

An effective information system leads the organization to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives. Information system auditor must know the characteristics of users of the information system and the decision-making environment in the auditee organization while evaluating the effectiveness of any system(Krishna Moorthy et al., 2011; Sarens & Abdolmohammadi, 2011).

Other study also constitutes on how information technology affects internal control (control environment, risk assessment, control activities, information and communication and monitoring) and provides guidelines and best practices in evaluating techniques available effectively perform auditing tasks internally. It also addresses how technology, Information system and electronic data processing have changed the way organizations conduct its business, promoting operational efficiency and aid decision-making(Krishna Moorthy et al., 2011).

Controls can be preventive, detective, or reactive, and they can have administrative, technical, and physical implementations. Examples of administrative implementations include items such as policies and processes. Technical implementations are the tools and software that logically enforce controls (such as passwords). Physical implementations include controls such as security personnel and locked door(Davis et al., 2011).

Internal audit effectiveness to the extent, which an internal audit office meets, its raison is arguably a result of the interplay among four factors: system audit quality; management support; organizational setting; and attributes of the audited. The management support with resources and commitment to implement the internal audit recommendations is essential in attaining audit effectiveness. In addition, the organizational setting in which internal audit operates, i.e. the organizational status of the office, its internal organization and the policies and procedures applying to each auditee, should enable smooth audits that lead to reaching useful audit findings. Further the capability, attitudes and level of cooperation of the auditee impact on the effectiveness of audits (Mihret & Yismaw, 2007).

The information system audit is an integral part of the internal audit process since it complements the auditor's role and supports his judgment on the quality of the information processed by computer systems(Majdalawieh and Zaghlou, 2009).

The migration of e-business tools and practices into government organizations is changing the way the citizens and governments interact. Governments are transforming themselves as they increasingly move to delivering information and services electronically; this is also the case in

Georgia. As a result, IT auditors are needed to provide assurance that systems are adequately controlled, secured and functioning as intended(Jackson & Harris, 2003).

Information technology audit has become an increasingly important issue in recent years. The increased role of information technology in society and organizations has increased the demand for IT audit. The purpose of this paper is to identify the role and necessity of IT audit in public sector organizations. Also to assess weaknesses and strengths of IT audit function and give some recommendation to improve IT audit performance, which will lead organizations to have much more effectively and efficiently in the exercise of their activity and to reduce as many risks(Beridze, 2017).

Banks, insurance companies and microfinance institutions are the major financial Institutions operating in Ethiopia. By the end of 2020/21, the number of banks reached 19,including the newly opened interest free bank(ZamZam bank) which opened 833 new branches during the review financial year, thereby raising the total number of bank branches to 7,344 from 6,511 last year(NBE, 2021). The banking industry is one of the most severely impacted service sectors, with significant capital invested in adopting new technologies. However, its implementation is still in its early stages in developing countries such as Ethiopia(Jerene & Sharma, 2020).

Technology is becoming increasingly important in Ethiopian banks. Banks have traditionally sought media through which they could serve their clients more cost-effectively while also increasing the utility of their clientele. Their primary concern has been to serve clients more conveniently while increasing profits and competitiveness. For many years, electronic and communication technologies have been extensively used in banking to advance the banking agenda (Abor, 2004). Years as time has passed, technology has advanced (and is still increasing). And banks have revolutionized the use of electronic innovations such as the Automated Teller Machine (ATM), telephone banking, personal computer banking, and internet banking, branch networking, and electronic funds transfer in their pursuit of providing convenient and improved services to their clients.

Another impediment to the adoption of new technology in the banking industry is the lack of a suitable legal and regulatory framework for e-commerce and e-payments. Ethiopia has yet to pass legislation addressing e-commerce concerns, such as the enforceability of the validity of electronic contracts, digital signatures, and intellectual property rights; it also restricts the use of encryption technologies and has high illiteracy rates. Low literacy rates are a significant barrier to the adoption of e-banking, which is problematic in Ethiopia because it limits access to banking services. Citizens must not only be able to read and write in order to fully enjoy and reap the benefits of e-banking, but they must also have basic ICT literacy (Gardachew 2010).

In Ethiopia, IT auditing is a newly emerging phenomenon. Thus, not much research has been done on the subject. A study has been conducted to assess Information System Audit effectiveness a case study on Commercial Bank of Ethiopia by (Tariku Demissie, 2018), aimed at identifying the success of Information System Audit. A study was also conducted by(Begashaw, 2018) (Begashaw, 2018) on factors affecting the quality of Information technology (IT) audit in Ethiopian Commercial Banks which aimed at exposing the influences that contribute to the quality of IT audit.

With growing nature of financial institutions the need for technological advancement also increases thereby, emergent risks of financial crimes require financial institutions to safeguard their financial information by all possible means.

There is likely to be variance in the scope of IT auditing across various corporate industry sectors, as well as variety in the obstacles that different banks experience in implementing effective IT audits. This study will investigate how these variances manifest themselves in commercial banks.

The researcher was motivated to evaluate the extent of IT auditing practices used by the auditors in an effort to ensure successful IT auditing.

1.3. Research Question

The study will be undertaken to address the following question:

1. What level of communication do IT auditors have with the IT department?
2. What is the level of IT audit engagement with technology projects?
3. Does the management, in collaboration with auditees, have support for an IT audit?
4. What extent of the IT audit framework is used in carrying out IT audit practice?
5. Are competent IT auditors available in the industry?
6. Do banks have the organizational structure in place to conduct an IT audit?
7. Is the management ready for IT security, privacy, cyber security, data management and governance, and emerging technology and infrastructure?

1.4. Objective of the study

1.4.1. General objective

The general objective of the study was to determine the extent to which IT auditors' practices met audit objectives in Ethiopian private commercial banks.

1.4.2. Specific Objective of the Study

The study has the following specific objectives.

1. To identify the level of communication of IT auditors with the IT department.
2. To identify the level of IT audit engagement with technology projects.
3. To evaluate the management support and collaboration of auditees towards executing IT audit.
4. To investigate the extent of the IT audit framework used in carrying out IT audit practice.
5. To evaluate the availability of competent IT auditors in the banking industry
6. To assess the organizational structure in order to carry out an IT audit.
7. To determine the levels reediness of the management for it security and privacy/cyber security data management and governance and emerging technology and infrastructure.

1.5. Significance of the study

The findings of this study will be used by Ethiopian banks to assess their performance in terms of IT auditing. The study will document the difficulties encountered in the effort to achieve successful auditing in Ethiopia's banking industry. The difficulties encountered in IT auditing will force auditors to be more prepared as they plan audits in Ethiopian banks.

Academics may use the study's findings as a foundation for future research in IT auditing. More academic research on IT auditing topics is expected to result from the findings of this study. A comparative study may be required to document the differences in IT audit among Ethiopia's various sectors.

The findings of this study will be of interest to professional bodies as an advisory organ in the provision of auditing guidelines and the development of an IT audit framework for Ethiopia. Understanding the scope of IT audit practice in banks would be beneficial in providing intelligent professional advice on how to improve IT auditing.

The National Bank of Ethiopia is in charge of regulating the banking industry in Ethiopia. IT auditing among financial institutions is one of the central bank's major concerns as part of stabilizing and improving efficiency in the banking sector, so the findings of this study would be of interest to the central bank.

The practice of IT audit in the banking industry would be of interest to government agencies and institutional bodies as well. This would be important information for Ethiopian policymakers when making IT-related choices. Because it involves the transfer of assets and money, implementing the IT policy and the e-government strategy papers would necessitate a functional e-commerce network. Because most systems have integrated technology, IT auditing can only verify the required IT compliance in the banking industry. As a result, the findings of the practice are valuable.

1.6. Scope of the Study

This study is limited to Information Technology audit practice in case of selected commercial banks in Ethiopia found in Addis Ababa.

1.7. Limitation of the study

Despite the researchers' best efforts to collect as much objective data as possible, the analysis of this study will be based on respondents' opinions, so respondents may not provide all of the required data. Because the banks kept these documents confidential, it was impossible to obtain policies and procedures related to the topic for this study, and the research found this to be a limitation for the study.

1.8. Organization of the study

This paper will be divided into four sections: The first chapter gives an overview of the research. It includes a background of the issues with which the study is concerned, an introduction, a problem statement, objectives, scope and limitations, and the study's organization. The second chapter evaluates previous literature and studies relevant to the field as well as related topics. The third chapter will describe the study's research methodology.

Chapter Two

II. Literature Review

2.1. Theoretical framework

In this section, the research aimed mainly to highlight the main concept of Information Technology and its components then move to the Information system definition and its type.

2.1.1. IT AUDIT

"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).

Today's global economies are more reliant on information technology, and IT-related risks have a greater impact on business operations, necessitating the need for strong IT controls for business operations, which necessitates IT auditing (Stoel, 2012).

An IT audit's primary function is to ensure the integrity of an organization's information systems (Harb, 2012).

Identifying and addressing risk is one of the most important issues in business, and IT is at the heart of any organization. The IT audit ensures that these risks are addressed as soon as possible and as thoroughly as possible. (Björklund, 2015).

The discovery of irregular acts, such as intentional violations of policies or regulations or unintentional violations of the law, is one aspect of conducting IT audits (Merhout, 2008).

In complex and dynamic business environments where IT is becoming increasingly important to organizations, the role of the internal audit function shifts from a traditional one focusing on accounting and financial control to a more strategic one focusing on risk management and corporate governance. The overall corporate governance applies to IT governance efforts as well to assist all employees and business functions including IT and its Governance of the organization to provide as much assistance as possible. (Bogale, Donald, & Prof., Auditing IT and IT Governance in Ethiopia , 2015).

2.1.2. IT and Auditing

The use of computer facilities has resulted in radically different methods of processing, recording, and controlling information, as well as the consolidation of many previously separate functions. As a result, the potential for material system error has increased significantly, resulting in significant costs to the organization. Because many computer applications are highly repetitive, small errors can result in large losses. This makes it critical for the auditor to test the invisible processes and identify the vulnerabilities in a computer system, as the costs associated with errors and irregularities can be enormous.

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

The Electronic Data Processing Auditors Association (EDPAA) was founded in 1960 by EDP auditors. The association's goal was to create guidelines, procedures, and standards for EDP audits. The first edition of Control Objectives was published in 1977. Control Objectives for Information and Related Technology (COBIT) is the new name for this publication. The EDPAA was renamed the Information Systems Audit and Control Association (ISACA) in 1994. From the late 1960s to the present, technology has changed rapidly, from the microcomputer and networking to the internet, and with these changes have come some major events that have altered traditional auditing methodologies.

2.1.3. Objectives of IT Audits

The goal of an IT audit is to assess a company's computerized information system to determine whether it produces timely, accurate, and reliable information outputs, as well as to ensure data confidentiality, integrity, availability, and reliability, and adherence to relevant legal and regulatory requirements (Parker, 2001). Understanding how well management capitalizes on the use of information technology to improve important business processes is one of the goals of conducting an IT audit as part of a financial audit statement.

IT auditing assists management in comprehending the pervasive impact of information technology on the client's critical business processes, such as the development of financial statements and the business risk associated with these processes. An IT audit assists management in determining the effectiveness of controls over information technology processes that have a direct and significant impact on financial data processing. When IT audit is included in a performance audit, the audit's objectives include ensuring that all aspects of the IT systems, including necessary controls, are effectively enforced.

Furthermore, IT audits ensure compliance with all applicable laws, because failure to comply and/or protect data exposes the organization to potential lawsuits, financial losses, and reputational harm (Riggins, 2016). IT audits look at how policies, plans, procedures, laws, and regulations are being followed. In this case, the audit function is in charge of determining whether the systems are adequate and effective, as well as whether the audited activities comply with the appropriate requirements.

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

Furthermore, IT audits pertaining to the economical and efficient use of resources should identify conditions such as underutilized facilities and nonproductive work. Procedures that are not cost justified, as well as overstaffing or understaffing, are the responsibility of management. Management is responsible for establishing operating or program objectives and goals, developing and implementing control procedures, and achieving desired operating or program results. The audit function should determine whether such objectives and goals are consistent with the organization's (Institute of Internal Auditors (IIA), 2000).

2.1.4. The Importance of IT Auditing

Computers play an important role in assisting the organization in data processing and decision making. It is critical that their use be controlled, because the rapidity of change and the amount of resources invested in IT from time to time complicates IT management activities (Bogale, Donald, & Prof., Auditing IT and IT Governance in Ethiopia , 2015) and the costs of errors and irregularities in these systems can be significant. Not only must they be controlled, but also the manner in which they are used and their impact on an organization's overall objectives must be assessed (OFAG, 2017). This calls for the auditor to become involved in supporting and assisting with the implementation of corporate governance in IT and management. (Bogale, Donald, & Prof., Auditing IT and IT Governance in Ethiopia , 2015).

IT audits are critical organizational processes that add value to the organization by providing assurance on the integrity, dependability, and quality of the information produced by the organization's information systems (Siew E. e., 2017). IT auditing is required to ensure that the data collected by systems is controllable, secure, and functional. The IT auditor is becoming increasingly important in assisting businesses in managing and responding to risks. (Björklund, 2015).

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

An IT audit should be performed by all industries, but it is especially important for banks and financial institutions. Furthermore, it is required by regulations to develop an information technology audit program to support its information technology infrastructure, to keep non-public customer information secure, and to conduct an annual risk-based audit (Lovaas, 2012).

2.1.5. IT Audit Scope

The scope of an IT audit is typically defined by a scoping document created near the beginning of the assignment. It typically refers to specific key risks of concern to management that revolve around computer and/or telecommunications systems. The scope of an audit assignment is typically a compromise between breadth (the range of issues to be reviewed) and depth (i.e. the amount of detail reviewed in each matter). Clever audit plans combine broadly scoped high-level audits (designed to identify the most critical risk areas) with narrowly scoped in-depth audits to provide a bit of both (Institute of Internal Auditors (IIA), 2000).

The scope of computer audit is difficult to define because it is dependent on the size and composition of the audit team: in large audit teams, computer audit may have a number of dedicated and specialized staff who are solely responsible for technology auditing. However, computer auditors are frequently expected to contribute to other types of audits (Institute of Internal Auditors (IIA), 2000).

2.1.6. Process of IT Auditing

Different audit organizations approach computer auditing in different ways, and individual auditors have preferred methods of operation. However, the following are the main stages of a typical computer audit assignment (Mr.Avadh Yadav, Information Technology Audit, n.d.).

1. Scoping and pre-audit survey -The auditor determines the main areas of focus and any areas that are explicitly out-of-scope, typically based on some form of risk-based assessment. At this stage, information sources include background reading and web browsing, previous audit reports, and, occasionally, subjective impressions that merit further investigation.

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

3. Fieldwork stage entails gathering evidence through interviews with employees and managers, reviewing documents, printouts, and data, and observing processes This step may include the use of Computer Aided Audit Techniques (CAATs) to assist in the analysis of IS systems and applications.

4. Analysis stage is about sorting through, reviewing, and attempting to make sense of all of the evidence gathered previously. It entails conducting a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis of the IT environment.

5. Reporting phase involves going over the analysis and trying to make sense of it before writing it up. The preliminary report is then circulated within the department for peer review before being modified again, circulated or presented to clients and client managers for feedback, and finally issued.

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

2.1.7. Information Technology Audit Types

2.1.7.1. General Control

Apply to all aspects of the IT function, including IT Administration; separation of duties; systems development; physical and online security over access to hardware, software, and related data; backup and contingency planning in the event of unexpected emergencies; and hardware controls. Because general control for the company as a whole. The six categories of general control have an entity wide effect on all IT functions. Auditors typically evaluate general control early in the audit because of their impact on Application controls (Arens et al., 2014).

- **Administration of the IT Function -**the board of directors and senior management's attitude about IT affect the perceived importance of IT within an organization. Their oversight, resource allocation, and involvement in key IT decision each signal the importance of IT. In complex environments, management may establish IT steering committee to help monitor the organization's technology needs. In less complex organizations, the board may rely on regular reporting by a Chief information officer (CIO) or other senior IT manager to keep management informed. In contrast, when management assigns technology issues exclusively to lower-level employees or outside consultants, an implied message sent that IT is not high priority. The result is often an understaffed, underfunded, and poorly controlled IT function.

- **Separation of IT Duties -**to respond to the risk of combining traditional custody, authorization, and record-keeping responsibilities by having the computer perform those tasks, well-controlled organization respond by separating key duties within IT. Ideally, responsibilities for IT management, systems development, operations, and data control should separate as follows:

- **IT management -The** CIO or IT manager should be responsible for oversight of the IT function to ensure that activities are carryout consistent with the IT strategic plan. A security administrator should monitor both physical and online access to hard ware, software, and data files and investigate all security breaches.

- **Systems development -**Systems analysts, who are responsible for the overall design of each application systems, coordinate the development and change of IT systems by IT personnel responsible for programming the application and personnel outside IT who will be the primary system user. Programmers develop flowchart for each new application, prepare computer instructions, test the programs, and document the results. Programmer should not have access to input data or computer operations to avoid using their knowledge of the system for personal benefit. They should allowed to work only with test copies of programs and data so they can only make software changes after proper authorization

- **Operations** computer operators are responsible for the day-to-day operations of the computer following the schedule establish by the CIO. They also monitor computer consoles for messages about computer efficiency and malfunctions. Network administrators also affect IT operations, as they are responsible for planning, implementing, and maintaining operations of the network of servers that link user to various applications and data files

- **Data control-**Data input/ output control personnel independently verify the quality of input and reasonableness of output. For organization the use of database to store information shared by accounting and other functions, database administrators are responsible for the operation and access security of shared databases.

- **Systems development-** There is various approaches to software development: traditional information systems development, purchasing and modifying a packaged system prototyping and rapid application development, and less formal end-user development. Although each approach is unique, they all have similar steps that must completed, For example, each approach will have to define user requirements, design programs to fulfill those requirements, verify that programs work as intended, and implement the system. Auditors need to understand the different approaches; the risks associated with a particular approach, and help ensure that all the necessary components are included in thedevelopment process.

A formal systems development process provides an environment that is conducive to successful systems development. This includes:

1. An information systems strategy that guides developers in building systems those areconsistent with the organization's technical and operational goals,
2. Standards that guide in the selection of hardware, software, and developing newsystems,
3. Policies and procedures that support the organization's goals and objectives, and
4. Project management that ensures projects completed on time and within budget. Auditors can assist organizations by reviewing the systems development process toensure that developed systems comply with the organization's strategy and standards(Fitzgerald & Peltier, 2016).

- **Physical and online security-** Physical control over computers restrictions to online software and related data files decrease the risk of unauthorized change to programs and improper use of programs and data files, Security plan should be in writing and monitored. Security controls include both physical controls and online access controls.

2.1.7.2. Physical controls

Proper physical control over computer equipment restrict access to hardware, software, and backup data file on magnetic tapes or disks, hard drivers, CDs, and external disks. Online access controls. Proper user IDs and passwords control access to software and related data files, reducing the likelihood that unauthorized changes made to software applications and data files. Separate add on security software packages, such as firewall and encryption programs, can be install to improve a system's security.

- **Backup and contingency planning** Power failures, fire, excessive heat or humidity, water damage, or even sabotage can have serious consequences to businesses using IT. To prevent data loss during power outages, many companies rely on battery backups or on site generators. For serious disasters, organizations need detailed backup and contingency plans such as off-site storage of critical software and data files or out sourcing to firms that specialize in secure data storage.

- **Hardware controls** Hardware controls built into computer equipment by manufactures to detect and report equipment failures. Auditors are more concerned with how the client handles errors identified by the hard ware controls than with their adequacy. Regardless of the quality of hardware controls, output will corrected only if the client has provided for handling machine errors (Arens et al., 2014).

2.1.7.3. Application controls

The following are two of the most common responses:

- Application controls are the automated controls, built into an application system, that help ensure the completeness, accuracy, timeliness and authorization of transaction processing for that application.

- Application controls are the activities (manual, automated or a combination thereof) that ensure the completeness, accuracy, timeliness and authorization of transaction processing for an application (ISACA, 2009).

Application controls can be broken down into three main categories: input, processing, and output control(Fitzgerald & Peltier, 2016).

- **Input Controls** An input control meant to minimize risks associated with data inputinto the system. Defining input requirements ensures that the method of capturing the data is appropriate for the type of data being input and how subsequently use. Performance problems and accuracy issues can introduced with non-appropriate methods for capturing data. Input controls ensure the authenticity, accuracy, completeness, and timeliness of data entered into an application. Authenticity ensured by limiting access at the screen and field level and requiring secondary approvals of transactions above a defined threshold. Accuracy ensured by edit checks that validate data entered before accepting the transaction for processing. Completeness ensured through error-handling procedures that provide logging, reporting, and correction of errors. Timeliness ensured through monitoring transaction flow, logging, and reporting exceptions.

- **Processing Controls** Processing controls ensure the accuracy, completeness, and timeliness of data during either batch or online processing. These controls help ensure that the data is accurately processed through the application and that no data is added, lost, or altered during processing.

- Output Controls Output controls ensure the integrity of output and the correct and timely distribution of the output produced. To be useful, information must be accurate and received in time to benefit decision-making. Output controls include procedures to verify if the data is complete, accurate, and properly recorded; procedures for report distribution and retention; and procedures for correct output errors. If outputs produced centrally, then conventional controls such as a security officer and distribution logs may be appropriate. If output distributed over a data communication network, control emphasis shifts to access controls for individual workstations. Access to reports should base on confidentiality.

- **Reconciliation** Output should verify against an independent source to verify accuracy. For example, transaction totals posted to the general ledger should be reconciled against the detailed balance due in the accounts receivable system. Data that is common to two or more applications should be reconciled to verify consistency. Often, applications developed over time using the same information for different purposes.

- **Distribution** of output is clearly defined and physical and logical access is limited to authorized personnel. The need for output should regularly review as reports mayrequest at the time an application is developed but may no longer be useful. In addition, the same information may be used for more than one system with different views, organization, and use.

- **Retention** Because storage space (computer and physical) is expensive, retention periods and storage requirements should defined for programs, data, and reports. Critical information should be stored securely (e.g., encrypted) and its destruction should be permanent and conducted in such a way as to prevent unauthorized viewing

2.2. Empirical Review

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

2.2.1. Effectiveness of Information system Audit

Information system audit is integral part (subpart) of internal audit process, so the measurement of internal audit effectiveness also used to measurement in information system audit effectiveness.

2.2.1.1. Professional Proficiency of information system Auditors

Appropriate staffing of an internal audit department and good management of the staff are keys to the effective operation of an internal audit. An audit requires a professional staff that collectively has the necessary education, training, experience and professional qualifications to conduct the full range of audits required by its mandate (Al-Twaijry et al., 2003). Auditors must comply with minimum continuing education requirements and professional standards published by their relevant professional organizations and the IIA (2008) and musthave a high level of education in order to be considered a human resource(Bou-Raad, 2000).

According to (Albrecht et al. 1999; Ratlitt 1996) the greater the professional qualifications of the internal auditors in a given department, defined by the length of their professional training, experience and educational level, the greater the effectiveness of this department. Professional competence can be obtained through a variety of ways such as on job training, formal internal and external training, staff rotation, encouragement of become a certified auditor in area such as (certification like CIA, CISA, CFE and ACCA), and experience sharing session among the auditors.

The internal audit guideline also states that the professional competence of each internal auditor as well as his/her motivation and continuing training are the perquisite for the effectiveness of the internal audit. This means each internal auditor must maintain the required knowledge, skills and abilities to conduct the audit activity.

2.2.1.2. Quality of Audit Work

Glazer and Jaenike (1998) argued that performing auditing work according to internal auditing standards contributes significantly to the effectiveness of auditing. (D'Silva & Ridley, 2007)found in the UK that complying with professional standards is the most important contributor to internal audit's benefit. Internal audit quality, which is demonstrated by the offices' capability to provide useful and it findings and recommendations, is one of the most prominent factors on which audit effectiveness in anchored. The performance standards of the IIA (1996) require the auditor to plan and perform the work such that he or she would be able to arrive at useful audit findings and forward recommendations of improvement. The office's ability to properly plan, perform and communicate the results of audits is proxy for audit quality. Therefore, audit quality is debatably a function of extensive staff expertise.

In general, formal auditing standards recognize that internal auditors also provide services regarding information other the financial reports. They require auditors to carry out their role objectively and in compliance with accepted criteria for professional practice, such that internal audit activity will evaluate and contribute to the improvement of risk management, control and governance using a systematic and disciplined approach.

This is important not only for compliance with legal requirements, but because the scope of an auditor's duties could involve the evaluation of areas in which a high level of judgment in involved, and audit reports may have a direct impact on the decisions or the course of acti0n adopted by management ; (Bou-Raad, 2000). It can thus argued that greater quality of internal audit work understood in terms of compliance with formal standards, as well as a high level of efficiency in the audit is planning and execution will improve the audit's effectiveness.

The internal audit guideline also states that internal auditors expected to comply with standards for the professional practices of internal auditing published by the institutes of internal auditors (IIA) to conduct quality audit work. It also states that the quality assurance and improvement program should cover all aspects of the internal audit activity and continuous monitoring of its effectiveness. Which includes ongoing internal monitoring and periodic internal and external quality assessments.

2.2.1.3. Organizational Independence

The organizational independence of internal audit department can be gained by means of reporting to levels within the organization that allow the internal audit department to perform its responsibilities free from interference, avoiding conflict of interest, having direct contact with the board and senior management, having unrestricted access to records and employees and departments. Appointment and removal of the head of internal audit not being under the direct control of executive management and not performing non-audit work.

The internal audit guideline also states that internal auditors shall be independent of the activities they audit and maintain an independent attitude to conduct the audit activity effectively and efficiently. Chartered institute of public finance and Accountancy (CIPFA); Worldwide professional standards and guidance ;International standards for the professional practice of internal Auditing (ISPPIA) and the institute of internal Audit (IIA); practice advisory suggestion(Gray & Abdolmohammadi, 2016).

2.2.1.4. Career and Advancement

Goodwin (2001) argued that, internationally, the practice of staffing the internal audit department with career auditors is becoming less common, with more organizations using the function as a training ground for future management personnel. This practice is design to help the organization train will rounded senior managers. Internal auditors perform a wide Varity of activities across different departments within the organization that gives them the opportunities to learn how these departments function and how they managed.

Furthermore, mangers that have had experience in internal auditing should have a better understanding of the importance of internal control. The ability to use internal audit-roles as a stepping-stone to managerial positions is seeing as one of the advantages of having an in house internal audit function rather than outsourcing internal audit activities. Albercht et al (1999) found that most participants perceived internal audit as a gateway to either a managerial position, or a career in internal auditing. According to(Goodwin, 2004), internal auditors who operate in settings with more organizational career opportunities will invest more effort in their work in order to increase their promotion opportunities than those with fewer opportunities for organizational advancement who will invest less effort in their work, reacting in a lower performance level. The degree to which internal auditing;

2.2.1.5. Top Management Support

Fernandez and Rainey (2006) argued, based on a trough literature review, that top management support and commitment to change play a crucial role in organizational renewal, as senior mangers' can mobilize the critical mass needed to follow through on efforts launched by one or more visionary thinkers. A number of empirical studies have found top management: support for quality works to be a key factor in its improvement (Dale & Duncalf, 2006). Given this, it is not surprising that management acceptance of and support for the internal audit function has long seen as critical issue to the success of internal audits function (Cohen & Sayag, 2010).

Numerous recent studies have shown that top management support for internal auditing is an important determinant of its effectiveness. Finding such support is, of course, an important metric. Internal audit departments must have adequate resources to hire and retain a sufficient number of high-quality employees, to maintain modern training and development methods, and to acquire and maintain physical resources(Cohen & Sayag, 2010).

2.2.2. 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. All at once, audit findings must be translated into vulnerabilities and business impacts that operating managers and senior management can understand.

- 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 less applied (Senft, 2008).
- 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(Hall A. James, 2008)

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

- Low competency of use of 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, 2019).

- The inadequacy of controls in developed applications is a major challenge in IT auditing. The application development process should consider the required level of security; however, many applications developed in many businesses deviate from the standard application development process and are not thoroughly tested, making them 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).

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

- 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.

Based on the above theoretical and empirical evidence, this study focuses on assessing the practices of an IT audit of selected commercial banks in Ethiopia.

Chapter Three

Research Methodology

3.1.Introduction

This section describes the processes and approaches used in conducting the research. It details the methods and data sources used, the research design and procedures, the sampling techniques, the data collection and analysis methods, and ethical considerations. It explains the purpose of the research and the research questions. It also explains the data sources and sampling techniques used, including the sample size and selection criteria. Additionally, it describes the data collection and analysis methods, including any software and statistical tests used.

3.2.Research Design

The research design is meant to provide a suitable framework for a study. The choice of research approach is a critical decision in the research design process because it determines how relevant information for a study will be obtained; however, the research design process involves many interrelated decisions (Aaker et al., 2013).

This study employs a mixed type of methods. The first part of the study consists of a series of well-structured questionnaires (For IT auditors of the internal audit department of the banks) and semi-structured interviews with key stakeholders (Chief internal auditor/director of internal audit department and IT audit manager) in participating banks.

Hence, this study employs a descriptive research design to agree on the practices of IT auditors in the banking industry. (Saunders et al., 2009) and (Fraenkel et al., 2012) say that descriptive research accurately portrays people, events, or situations. This design provides researchers with a profile of described relevant aspects of the phenomenon of interest from an individual, organizational, and industry-oriented standpoint. Therefore, this research design has enabled the researcher to gather data from a wide range of respondents on the practice of IT audit in Ethiopian private banks. And this helps in analyzing the response to be obtained from the banking industry.

3.3.Research Approach

To address the key research objectives, this research has used both qualitative and quantitative research approach .The qualitative data supports the quantitative data analysis and results. The result obtained has triangulated since the researcher has utilized qualitative and quantitative data types in the data analysis.

3.4.Data sources

Primary data was obtained from the original source of information. The primary data is more reliable and has a higher level of confidence in decision-making because the trusted analysis has a direct correlation with the occurrence of the events. Through questionnaires and interviews, the primary data sources are the bank's IT audit staff (IT audit management and officers) and the internal audit department directors.

3.5.Sampling Approach

3.5.1. Target population and sample size determination

The study population consisted of 16 Private Banks operating in Ethiopia. To select representative purposive sampling is considered. For the questionnaire survey, 41 sample sizes of internal audit departments of bank respondents were identified from the priority areas of IT audit. Currently, 30 banks are operating in Ethiopia, according to the(NBE, 2022) as of June 30, 2022. From among the 30 banks currently operating, two of them are government-owned, and the remaining 12 are young in business or have 1 year or less of operation, thus the researcher took a sample of 16 private banks that have been operating for more than a year. A list of the selected banks is depicted in the following table:

Table 1: Target Population

S.no.	Name of banks	Year of Establishment	Number of IT auditors
1.	Awash international Bank S.C	1994	4
2.	Dashen Bank S.C	1995	4
3.	Bank of Abyssinia S.C	1996	4
4.	Wegagen bank S.C	1997	3
5.	United Bank S.C	1998	2
6.	Nib International S.C	1999	0
7.	Cooperative Bank of Oromia S.C	2005	3
8.	Lion international Bank S.C	2006	2
9.	Oromia International Bank S.C	2008	2
10.	Bunna International Bank S.C	2009	3
11.	Zemen Bank S.C	2009	2
12.	Abay International Bank S.C	2010	4
13.	Berhan International Bank S.C	2010	3
14.	Addis International Bank S.C	2011	2
15.	Debub Global Bank	2012	2
16.	Enat Bank	2013	1
Total			**41**

Source: National Bank of Ethiopia

3.5.2. Questionnaire sample size determination

The sample size for the questionnaire was determined to have enough respondents to ensure that the results of the survey are statistically significant. To determine the right sample size, purposive sampling was used by considering the population to be represented, the level of accuracy needed, and the amount of variability expected. By taking these factors into account, all information technology auditors on the targeted 16 banks, totaling 41, were selected to ensure a meaningful result that accurately represented

3.6.Data collection methods

The following fundamental techniques are used to collect data: As defined in the previous section, this includes primary data collection focusing on both qualitative and quantitative data. The data collection mechanisms have been designed and are ready with their associated procedures. Primary data sources include both qualitative and quantitative information. Interviews are the qualitative sources, while survey questionnaires are the quantitative sources.

3.6.1. Data collection through interview

An interview is a loosely structured qualitative in-depth interview with people who are thought to be particularly knowledgeable about the subject under consideration. The semi-structured interview is typically conducted face-to-face, allowing the researcher to seek new insights, ask questions, and assess phenomena from various perspectives. It provided detailed information to the researcher about the current working environment, its influential factors, and its consequences. It has allowed for the refinement of data collection efforts as well as the examination of specialized systems or processes. It was used when the researcher was constrained by written records or published documents, or when the researcher wanted to triangulate data obtained from other primary and secondary data sources.

This paper is also written in a qualitative approach and includes interviews. The benefit of using interviews as a method is that respondents can raise issues that the interviewer may not have anticipated. The corresponding researcher conducted all face-to-face interviews with chief audit executives and IT audit managers at their workplace.

3.6.2. Data collection through questionnaires

Since the researcher can choose the sample and the types of questions to be asked, questionnaires are the primary tool for gathering primary information in practical research(Saunders et al., 2009).

In this survey, each respondent is asked to answer an identical list of questions mixed together to avoid bias. As a result, the questionnaire generated valuable data that was required to meet the thesis objectives.

The questionnaire was created using a five-item Likert scale. Each statement received a five-point Likert-type scale response, with 1 indicating "strongly disagree" and 5 indicating "strongly agree." The responses were totaled to generate a score for the measures. The proposed data source received a high response rate, and the pilot test demonstrated the reliability of questionnaires.

The questionnaire data was entered into Microsoft Excel, where it was edited, coded, and tabulated based on the variables. The data was then analyzed and presented using tabulation, graphs, and charts in the statistical Package for Social Sciences (SPSS) software (version 22).

According to(Abdelrasheed, n.d.), the mean cut-off point for the 5-level Likert scale is said to be very low when the mean is 1 to 1.8; low between 1.8 and 2.60; moderate: 2.60-3.40; high: 3.40-4.20; and very high: 4.20-5.00, which could be interpreted as respondents disagreeing from 1 to 2.6, neutral from 2.6 to 3.4, and agreement from respondents above 3.4.

3.6.3. Data Analysis and Presentation

3.6.4. Data Analysis

Data analysis method follows the procedures listed under the following sections. The data analysis part answered the basic questions raised in the problem statement.

3.6.5. Quantitative data analysis

Quantitative data was obtained from primary data discussed above in this chapter. This data analysis has used IBM SPSS data analysis tool. This data analysis focuses on numerical/quantitative data analysis. Under the data analysis, exploration of data was made with descriptive analysis.

3.6.5.1. Qualitative data analysis

The quantitative data analysis was triangulated using qualitative data analysis. The findings were supported by the interview. In the data analysis sections, the analysis is combined with the quantitative discussion results.

The overall flow of the research for the given study is indicated by the research methodology and design.

3.6.6. Data Presentation

The researcher primarily used tables to present the quantitative primary data collected from the IT auditors' questionnaires. In-depth discussions and expositions were also used in the study to present the qualitative data gathered from key informant interviews with the bank's internal audit directors and IT audit managers.

3.6.7. Research Reliability

This issue concerns whether research findings can be applied to a larger group than those who participated in a study. Reliability is primarily concerned with ensuring that data collection methods produce consistent results. This can be measured in some types of research by having different researchers use the same methods to see if the results can be replicated. If the results are similar, the data collection method is most likely reliable. Assuring that research can be replicated and produce comparable results is a critical component of the scientific research method. (https://www.knowthis.com/marketing-tutorials/marketing-research/#research-validity-and-reliability)

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 (0.758) indicated that the survey questionnaire is reliable since it is greater than 0.7 which is the minimal alpha value as depicted in the following table

Table 2: Reliability Test

Cronbach's Alpha	N of Items
0.758	49

3.6.8. Ethical Considerations

The researcher followed ethical norms as much as possible during data collection in order for the research process to run smoothly. Based on this statement, the researcher required a written recommendation from the academic authority of Saint Mary's University's School of Graduate Studies, which was then presented to the appropriate office for approval to collect all necessary information from the intended field. Meanwhile, it was up to the researcher to reassure all respondents that any information they provided would be treated and guarded with strict confidentiality and that no part of it would be revealed.

Chapter Four

Presentation of Results and Discussion

This chapter provides a detailed overview of the research and results of the study. It includes a description of the methods and materials used, a clear presentation of the results, and an in-depth discussion of the findings.

It explains the implications of the results and provides a comparison to other studies in the field. It also provides a critical analysis of the data and any limitations of the study.

Furthermore, it includes a conclusion summarizing the main findings and recommendations. Therefore, the data analysis for each grouped questionnaire was described as follows

4.1. Descriptive Statistics Result

4.1.1. Response rate of respondents

The questionnaires were distributed to the information technology auditor managers and other information technology auditors at 16 purposefully selected Ethiopian private commercial banks. 41 questionnaires (a total of 57 questions) were delivered to each staff member. From the distribution of 41 questionnaires, 41 questionnaires were collected (16 responses from IT audit managers and 25 other responses from IT audit staff), giving a response rate of 100%. This shows a good response rate for all respondents.

4.1.2. Response rate of interview

Nine chief internal audit executives were interviewed from the 16 purposively sampled commercial banks operating in Ethiopia, yielding a 63% response rate, which is satisfactory for all respondents.

4.1.3. Demographic Profile of Respondents

The effectiveness of an internal audit function will depend on the competence of the internal audit staff (Burnaby, et al., 2009; Cohen and Sayag, 2010; Belay 2007). In this respect, the researcher attempted to look into the competence of the Information technology audit staffs as presented under below.

As can be seen from Table 3, all of the respondents have at least a first degree and a master's degree, and most of them have over five years' experience in the banking industry and over two years of IT auditing experience. Over 70% of the respondents have an information systems background. All of them secured their profession-related certificates after joining the banking industry, which reveals that banks are engaged in the continuous improvement of their staffs' expertise on the specific subject matter that adds value to the success of their operation.

Table 3: Respondents' profile

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Education Level					
Valid	Bachelor‘s Degree Level	24	58.5	58.5	58.5
	Masters Level	17	41.5	41.5	100
	Total	41	100	100	
Banking Experience					
Valid	Less than 2 years	6	14.6	14.6	14.6
	2-5 years	18	43.9	43.9	58.5
	6-10 years	17	41.5	41.5	100
	Total	41	100	100	
IT Auditing Experience					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 2 years	12	29.3	29.3	29.3
	2-5 years	23	56.1	56.1	85.4
	6-10 years	6	14.6	14.6	100
	Total	41	100	100	
Qualification					
Valid	Accounting and finance	12	29.3	29.3	29.3
	Information technology	29	70.7	70.7	100
	Total	41	100	100	
Certification					
Valid	CIA	6	14.6	17.1	17.1
	CISA	6	14.6	17.1	34.3
	CISSP	11	26.8	31.4	65.7
	Other	12	29.3	34.3	100
	Total	35	85.4	100	
Missing	System	6	14.6		
Total		41	100		
Career post					
Valid	IT audit staff	25	60.97	60.97	60.97
	IT audit manager	16	39.02	39.02	100
	Total	41	100	100	
Certificates earned after joining the bank					
Valid	CIA	6	14.6	17.1	17.1
	CISA	6	14.6	17.1	34.3

		Frequency	Percent	Valid Percent	Cumulative Percent
	CISSP	11	26.8	31.4	65.7
	Other	12	29.3	34.3	100
	Total	35	85.4	100	
Missing	System	6	14.6		
Total		41	100		

Source: Own Survey

4.1.4. Communication with the IT department

According to the first section of the questionnaire (Q1-Q4), which examines the communication of IT auditors with the IT department, there was a mean response of less than 2.5. This implies that participants have agreed on the communication with committees (working groups) that the IT department invites IT audit to participate in. Based on the results and the researcher's understanding of the value that such communication can deliver, it is concluded that the aggregate mean response of 2.87 reveals that the respondents remained neutral on the effectiveness of the communication of IT auditors with the IT department. As the bank's IT department undertakes more strategic technology projects, a formal process to assess and potentially halt these projects if new risks are identified becomes more important. IT audit participation in IT governance and risk management committees is less likely, but there is value in having IT audit participate in these other working groups as well.

However, the one-to-one interview revealed that IT auditors are not adequately informed as expected. IT auditors need to have effective communication with the IT department in order to ensure the accuracy of the information they are auditing. The communication between the two parties should be professional, clear and concise, so that everyone involved is aware of their responsibilities and expectations.

IT department should also be proactive in their communication keeping The IT auditor any changes that occur during the process, as well as any new information that could be relevant to the audit. This will help the IT audit to be prepared for issues that may arise.

This is important to ensure that any changes that were made during the audit process have been implemented correctly and that the audit was successful. Following up also allows the IT auditor to hear any feedback from the IT department regarding the audit process and to make any necessary changes or adjustments for the next audit.

By taking the time to properly communicate with the IT department, IT auditors can ensure that their audit is effective and successful. This will benefit both the IT auditor and the IT department, as it will ensure that the audit process is completed accurately and efficiently.

Table 4 : Communication with the IT department

	N	Sum	Mean	Std. Deviation
IT auditors collaborate in the strategic technology project of the bank	41	106.0	2.585	1.4487
A formal process exists to continue or postpone the IT implementation of strategic technology projects if new risks emerge during the implementation process	41	164.0	4.000	1.0724
Committees/working groups that the IT department invites IT audit to participate in technology projects	41	100.0	2.439	1.1842
The frequency with which the bank's process for identifying and assessing technology risk is carried out	41	86.0	2.098	1.0441
Valid N (list wise)	41			
Aggregate Mean			2.7805	

Source: Own Survey

4.1.5. IT audit engagement with technology projects

In this manner, respondents were asked to reflect on their opinions regarding their engagement with technology projects within their banks. Respondents have agreed with a mean value ranging between 2.0 and 2.2 that IT audits have minimal involvement in major technological projects from the planning to the designing and implementation stages. On the other hand, respondents with a mean value of 3.5 agreed that IT auditors are invited to participate in the post-implementation of technological projects.

The aggregate mean value of 2.54 indicated auditors had an insignificant impact on technology projects within their bank since they weren’t brought into technology projects until post-implementation.

Further, the one-on-one interview revealed that strategic technology projects at the banks do not sufficiently involve collaboration with the IT audit function. The IT audit team should work closely with the project teams to review the project's design, code, and documentation to ensure that it meets the necessary security and compliance requirements. Even though the IT audit team helps identify any potential risks associated with the project as well as any areas where the project could benefit from additional testing or review, IT auditors are not invited to these projects' inception.

Table 5: IT audit engagement with technology projects

	N	Sum	Mean	Std. Deviation
IT audit involvement have strategic technology projects on planning stage	41	82.0	2.000	1.2042
IT audit involvement have strategic technology projects on Design	41	120.0	2.927	1.5873
IT audit involvement have strategic technology projects on Testing	41	82.0	2.000	1.2042
IT audit involvement have strategic technology projects on Implementation	41	93.0	2.268	1.1186
IT audit involvement have strategic technology projects on Post implementation	41	144.0	3.512	1.0030
Valid N (list wise)	41			
Aggregate Mean			2.5415	

Source: Own Survey

This result is inconsistent with the explanation that says internal auditors can add significant value to a project by involving themselves early in the process and assisting the project team throughout the project's life cycle (Karine Wegrzynowicz, Lafarge SA Steven Stein & March, 2009).

4.1.6. Resource/Staffing/Skills Challenges

The mean level of 1.39 for questions 1 and 4 in this category indicates that IT auditors believe there is insufficient manpower to conduct IT audits in banks. Concurrently, auditors indicate an increased expectation of expertise across a broader subject area. With this shortage of skilled personnel, an IT audit team will be unable to meet the challenges of automation. The idea that the IT audit team should be supplemented with data scientists is somewhat contradictory or perhaps an outgrowth of that expectation.

Many auditors stated that they were unable to adequately address the issues raised by IT audits with a high degree of confidence due to a technical skills gap. IT audits are performed by full-time internal audit professionals in the internal audit department who specialize in IT audit projects. According to the responses to questions 3 and 7, banks make trainings more convenient by inviting outside trainers. The aggregate mean response of 2.42 reveals that the respondents disagree with the availability of the required resources and skills in the banking industry.

Furthermore, the one-on-one interview revealed that, given the current state of IT auditors, who are not highly experienced or knowledgeable in their field, they were unable to find a sufficient number of IT auditors in their banks or the market.

The result is in agreement with the survey conducted by (Protiviti.com, 2019)which states from an IT auditing standpoint as well as a broader IT standpoint, resource needs are changing, and organizations are challenged to bring in and retain the resources they require.

Table 6 : Resource/Staffing/Skills Challenges

	N	Sum	Mean	Std. Deviation
Enough IT auditors are available in the bank.	41	57.0	1.390	.4939
There are different aspects of your present IT audit plan that you are unable to adequately address due to a lack of resources or expertise.	41	176.0	4.293	.6420
IT audits are performed by full-time internal audit professionals in the internal audit department who specialize in IT audit projects.	41	125.0	3.049	.8047

	N	Sum	Mean	Std. Deviation
There are sufficient numbers of IT auditors available in the market with the required level of expertise to carry out quality audit work.	41	57.0	1.390	.4939
Your bank assists you in continuing to learn/train/obtain certificates in your field of expertise/specialization in IT auditing	41	57.0	1.390	.4939
The bank facilitates the trainings: In-house trainers	41	59.0	1.439	.5024
The bank facilitates the trainings: Outside trainers	41	164.0	4.000	.4472
Valid N (list wise)	41			
Aggregate Mean			2.4216	

Source: Own Survey

4.1.7. Management support

Boards remain significantly engaged with information technology issues the banks faces. This could indicate greater awareness among board members of organizational efforts to combat information technology threats. The 2.2 mean result of the question no.2 of this section. However, from the respondents' result of an aggregate mean value of 2.7, it could not be concluded that sufficient management support is obtained or not by IT auditors.

However, the one-on-one interview revealed that, due to the management's lack of technical expertise, the IT audit team is not provided with adequate feedback during the audit process. The management is responsible for ensuring that any issues that are identified are addressed in a timely manner and that any recommendations made by the audit team are implemented. This feedback is essential to ensuring that the IT audit process is as successful and effective as possible. By providing the necessary support and resources to the IT audit team, the management can help ensure a successful audit process.

Table 7: Management support

	N	Sum	Mean	Std. Deviation
Your bank's board of directors engage and understand information risk relating to your business	41	130.0	3.171	1.4301
Board of directors (Specifically audit committee) have technical expertise in relation with IT audit	41	92.0	2.244	1.4453
Valid N (list wise)	41			
Aggregate Mean			2.7073	

Source: Own Survey

Greater business knowledge will likely increase the relevance and practicality of IT audit findings and recommendations, in that they will address business impacts in terms that can be understood and assessed by management and others not possessing a detailed understanding of technology(*Business Skills for the IT Audit and Assurance Professional*, 2010).

4.1.8. Accepted industry framework employed

The mean response to questions 1-2, which examine the accepted industry frameworks used in banks, ranged from 2.2 to 3.2. This implies that participants disagreement that sufficient frameworks are being developed to carry out successful IT audit work.

Furthermore, the aggregate mean value of 2.7 shows respondents' indifference toward adequate IT audit framework development meeting international standards, which complicates the successful execution of an IT audit.

However, the one-to-one interview revealed that the current policy and procedures the banks are using are not up-to-date and tailored to their specific environment and risk profile.

It is essential for banks to have an effective IT audit framework in place to ensure that their systems and processes are secure and compliant with industry regulations. It is important for banks to review and update their IT audit frameworks regularly to ensure they are comprehensive and up-to-date. An effective IT audit framework should have the ability to accurately identify risks, evaluate controls, and provide assurance that the systems are working as intended.

Table 8: Framework employed

	N	Sum	Mean	Std. Deviation
Adequate frameworks are developed to carry out successful IT audit work	41	130.0	3.171	1.4301
The IT audits framework are developed in accordance with/meets international standards.	41	92.0	2.244	1.4453
Valid N (list wise)	41			
Aggregate Mean			2.7073	

Source: Own Survey

As mentioned in (Nicho & Muamaar, 2016) Several studies have reported challenges of implementing IT frameworks. Othman et al. (2011b)) found that the challenges of implementing ITG Frameworks included lack of top management support, communication, slack resources, centralization, formalization, industry/vendor support, regulatory environment, perceived benefits, and compatibility with existing Frameworks; complexity in the understanding and use of these frameworks; cost of new requirements; resistance to change; national culture; and politics. Another study revealed the challenges as change management, communication issues, lack of senior management commitment and support, difficulties in demonstrating value and benefits, difficulties in obtaining the required business participation, ineffective current enterprise governance, high level of organization complexity, and trying to accomplish multiple tasks simultaneously (I. ISACA, 2011).

During the same period, another study on five public sector organizations in Tanzania revealed that the top five issues inhibiting the adoption of ITG Frameworks include low acceptance of new IT applications and uses by business people; weak measurement of IT performance and value to business; inadequately defined IT-related roles, responsibilities, and accountability; insufficient staff members; and inadequate IT skills and competency (Othman et al., 2011b).

Since ITG frameworks overlap, this leads to implementation difficulties preventing organizations from adopting them (Nicho & Muamaar, 2016). Moreover, researchers found that the main issue concerning implementation challenges was related to organizations' internal and external factors, such as organizational culture and structure, strategy, size, regional differences, industry, maturity, ethics, and trust. Meanwhile, the most important contingent factors influencing ITG framework implementation are culture, structure, and industry (Pereira & Mira da Silva, 2012).

4.1.9. IT Security and Privacy/Cybersecurity

Respondents to the survey, with a mean value ranging from 3.4 to 3.8, agreed that establishing a stronger cybersecurity culture will increase their banks' profitability or viability. And the top management and boards of the banks are paying greater attention and becoming more involved with information technology risk. Furthermore, of the respondents, the mean value of 2.04 to 2.6 said there is a "significant gap" between their banks' current and desired cybersecurity culture and the needed technical expertise level to combat this security issue. In general, the aggregate mean value of 3.43 in this section indicates the respondents' agreement that IT security and privacy/cybersecurity are major challenges for bank IT auditors.

Furthermore, because their banks are changing and evolving as a result of numerous digital transformation efforts, IT auditors and professionals around the banks are likely to see security and privacy issues as the most pressing technology challenge.

Furthermore, the one-on-one interview uncovers that IT security and privacy/cybersecurity are major challenges for bank IT audit professionals. As technology advances and more data is stored and shared online, banks must take precautions to ensure their IT systems are secure and private. Encryption, secure authentication, and strong access control measures are all part of this. Furthermore, IT auditors must stay current on current security trends and threats to ensure their organization's security. Auditors must be aware of the risks associated with data breaches, phishing attacks, and other malicious activities. They must also maintain vigilance in testing and monitoring IT systems and networks to ensure that they are regularly updated and meet regulatory and industry standards.

Table 9: IT Security and Privacy/Cybersecurity

	N	Sum	Mean	Std. Deviation
Recent press coverage on cyber warfare and/or cybersecurity has affected your interest in and focuses on the subject of information security.	41	157.0	3.829	1.3766
The board of directors is involved with information security risks relating to the bank.	41	157.0	3.829	1.3766
The board of directors of the bank is adding technical expertise to the board and disclosure committee.	41	108.0	2.634	1.3740
Cybersecurity is included in the audit plan.	41	141.0	3.439	1.3048
Cyber-related audit activities have been performed.	41	141.0	3.439	1.3048
Cybersecurity audits are typically resourced Exclusively with in-house (IT audit) resources	41	149.0	3.634	1.1781
Cybersecurity audits are typically resourced In-house resources with support from technical	41	84.0	2.049	1.2237
Cybersecurity audits are typically resourced IT/information security resources	41	141.0	3.439	1.3048
Valid N (list wise)	41			
Aggregate Mean			3.4329	

Source: Own Survey

This result is consistent with the (Protiviti.com, 2019) survey, which stated that cybersecurity, as well as data security and privacy, remain top priorities not only for IT audit leaders but also for their organizations' boards of directors and management.

4.1.10.Data Management and Governance

As demonstrated by the response to question no. 2 with a mean result of 3.63 by the respondents in this section, banks examine the source of their data and ensure that clear rules and policies are in place to ensure that it is clean and usable.

According to the mean responses of 1.36 among respondents, most banks do not regard their data as a valuable asset because they do not pay close attention to how it is collected. The mean level of 1.43 of question no. 3 indicates, however, that IT auditors are not sufficiently empowered to access and govern the data being used to ensure various control and compliance requirements are met.

Overall, the aggregate mean result of 1.81 indicates that the bank's data management and governance practices are deficient.

Furthermore, the one-on-one interview indicates data management and governance are major challenges for IT audits. An IT audit must evaluate the effectiveness of the data management and governance processes to ensure that the data is managed and used in accordance with best practices. An IT audit must also ensure that data is properly secured and protected from unauthorized access and use. Additionally, an IT audit must review the data governance processes to ensure that any changes to the data are properly tracked and documented. An IT audit must review the data management and governance processes to ensure that data is being used in a manner that is compliant with applicable laws and regulations.

Table 10: Data Management and Governance

	N	Sum	Mean	Std. Deviation
Banks do not devote sufficient attention to how data is collected.	41	56.0	1.366	.4877
Banks look at the source of their data and make sure there are clear rules and policies in place that ensure it is clean and usable.	41	108.0	3.634	1.2798
IT audit is able to access and govern the data being used to ensure various control and compliance requirements are being met.	41	59.0	1.439	.5024
Valid N (list wise)	41			
Aggregate Mean			1.8130	

Source: Own Survey

4.1.11.Emerging Technology and Infrastructure Changes — Transformation, Innovation, Disruptions

Question no.1 and no.4 of this category have received a 4.1 and 4.2 mean level of response, respectively, which indicates that risk management practices and control structures, together with recovery systems, are in place within the banks to address emerging technology and infrastructure changes. However, the mean level of 1.8 of the answer to question no. 2

elaborates that even if the banks currently have risk management practices and control structures, they don't have a long-term strategy to transform IT audit into a data-driven function that makes use of leading technology solutions. The aggregate, mean level of 3.4 revealed that the respondents strongly believe that for banks to receive more efficient audits, deeper insights, and increased risk assurance, a similar level of data and technology enablement is expected within IT audit.

Furthermore, the one-on-one interview it's indicated that from digital transformations to disruptive innovations, IT auditors must be prepared to handle the challenges that come with the rapid changes taking place in the banking industry. Additionally, IT auditors must stay up-to-date on the latest technologies and standards to ensure that banks are taking advantage of the best solutions in the marketplace. Auditors must stay up-to-date on the latest technologies and regulations and be prepared to assess the risks associated with new technologies. By taking a proactive approach to auditing, IT auditors can ensure that banks are taking advantage of the best solutions in the marketplace and providing a secure and compliant service to their customers.

Table 11: Emerging Technology and Infrastructure

	N	Sum	Mean	Std. Deviation
Risk management practices and control structures are in place to address emerging technology and infrastructure changes.	41	168.0	4.098	.8002
The bank has a long-term strategy to transform IT audit into a data-driven function that makes use of leading technology solutions.	41	77.0	1.878	1.0769
For banks to receive more efficient audits, deeper insights, and increased risk assurance, a similar level of data and technology enablement is expected within IT audit.	41	139.0	3.390	1.6106
Data recovery system emplaced.	41	174.0	4.244	.7675
Valid N (list wise)	41			
Aggregate Mean			3.4024	

Source: Own Survey

This is inconsistence with the study conducted by(Thottoli et al., 2022) The presence of significant technological challenges has a significant and positive impact on auditing practice. This is demonstrated by the fact that practicing auditors face significant technological challenges in their auditing practice. If there is a high level of technological challenge, newly qualified auditors are ready to accept these challenges and use advanced technology tools for audit practice. This could be due to a variety of factors, including the belief among young, qualified auditors that customized audit software that is affordable for small-scale audit firms, combined with technology-based audit training, increases firm profitability and that technology-enabled auditing is understandable by anyone with a basic level of computer knowledge.

4.1.12.Structure of IT audit

Question 1, 2, and 9 received a mean response of 4.6, indicating agreement that banks have a designated IT audit manager in their internal audit departments, and the IT audit manager reports to the Chief Audit Executive in these banks. However, the mean response of 2.31 indicated the IT audit manager's disagreement about attending regular audit committee meetings to elaborate on a technical expertise skill, even though the chief audit executive is not knowledgeable enough to undertake a discussion with the audit committee about IT audit issues in depth. The 2.81 aggregate mean result of the respondents in this section shows respondents' indifference regarding the reporting line and that internal audit directors are knowledgeable enough to undertake a discussion with the audit committee about IT audit issues.

However, the one-on-one interview reveals that IT auditors in banks are commonly embedded within the internal audit department and report to the board's audit subcommittee through the internal audit director. Thus, instead of the IT audit manager or staff, internal audit directors usually report to the subcommittee with less necessary technical expertise and elaboration on the findings to get the necessary attention and subsequent actions.

Table 12: Structure of IT audit

	N	Sum	Mean	Std. Deviation
A designated IT audit manager (or equivalent position) exists in your bank.	41	189.0	4.610	.4939
Your bank's IT audit director/manger report to Chief audit executive	41	189.0	4.610	.4939
Your bank's IT audit director/manger report to Chief executive officer	41	57.0	1.390	.4939
Your bank's IT audit director/manger Report through some other function	41	66.0	1.610	.4939
Your bank's IT audit director/manger report to a director under the CAE	41	96.0	2.341	.9902
Your bank's IT audit director/manger report to a Chief information officer	41	107.0	2.610	1.4121
IT audit manager (or equivalent position) regularly attends the audit committee meetings.	41	95.0	2.317	.9602
The CAE is knowledgeable enough to undertake a discussion with the audit committee about IT audit issues	41	95.0	2.317	.9602
The organizational structure of your bank's IT audit resources; Part of the internal audit department not a separate function	41	189.0	4.610	.4939
The organizational structure of your bank's IT audit resources; Part of the internal audit department but considered to a separate function	41	107.0	2.610	1.4121
The organizational structure of your bank's IT audit resources; Embedded in the bank as a separate audit function	41	57.0	1.390	.4939
The organizational structure of your bank's IT audit resources; No IT audit resources are available within the bank	41	95.0	2.317	.9602
The IT audit is supported with outside resources to supplement or provide your IT skills	41	180.0	4.390	.4939
The IT audit hours covered by outside IT audit resource is more compared to the total IT audit hour	41	95.0	2.317	.9602
Valid N (list wise)	41			
Aggregate Mean			2.8171	

Source: Own Survey

Chapter Five

Summary, Conclusions and Recommendations

In this chapter the major findings of the study are summarized; conclusions are drawn based on the findings and recommendations are forwarded accordingly.

5.1.Summary of Major Findings

Summary of major findings of the study results from both primary data sources are presented as follows:

- There is communication challenge between IT auditors and IT departments within the banks.
- IT auditors have an insignificant impact on technology projects within their bank as they are not invited to participate on these projects.
- There is a shortage of skilled manpower to conduct IT audits in banks.
- The board of directors (Specifically audit committee) of these banks lack technical expertise in relation with IT audit.
- Insufficient frameworks which do not meet international standards are being developed to carry out successful IT audit work within the banks.
- IT auditors and professionals around the banks are likely to see security and privacy issues as the most pressing technology challenge.
- IT auditors are not sufficiently enabled to access and govern the data being used to ensure various control and compliance requirements are met.
- Banks lack a long-term strategy for transforming IT audit into a data-driven function that employs cutting-edge technology solutions. Banks are expected to deploy a similar level of data and technology enablement within IT audit to drive the delivery of more efficient

audits, deeper insights, and increased risk assurance as they pursue digital transformation with increasing zeal.

- Even if information technology audit function is in place in all the sampled banks, IT auditors are not attending regular audit committee meetings to elaborate on a technical expertise skill. Moreover the chief audit executives are not knowledgeable enough to undertake a discussion with the audit committee about IT audit issues in depth.

5.2.Conclusion

This study has assessed the practice of information technology auditing at 16 selected privately owned Ethiopian commercial banks. The researcher employed a questioner and a face-to-face interview as primary data.

From the summary of the research findings, all auditors that are engaged in IT audit are competent enough in terms of educational level, field of study, and work experiences in managerial or supervisory positions; all are members of the internal audit department.

However, the majority of information technology auditors within these banks have faced challenges such as a communication barrier with the IT department, failure to attend regular audit committee meetings to elaborate on a technical expertise skill for the audit committee, no long-term strategy to transform IT audit into a data-driven function, failure to engage in technological projects, a shortage of skilled manpower to conduct IT audits, and security and privacy challenges.

IT audits lack the ability to participate in planning discussions and provide additional critical perspectives such as risk identification and mitigation that can contribute to project success. This collaboration allows IT Audit to create a better audit plan and facilitate regular risk assessments. The same principle applies to regular risk assessments.

By being aware of events such as new applications being introduced or pushed into the network, IT audit can react quickly to provide relevant information as well as identify and alert on threats that IT needs to know about. More importantly, these actions can be taken in advance and not in response to requests or information previously unknown to IT Audit.

In terms of reporting results and recommendations to the board (including the audit committee) and management (a strong partnership with IT enables IT to provide better and more meaningful recommendations pertaining to strategic technology projects and other important On the other hand, when implemented in real life, the lack of effective collaboration between IT audit and the IT organization potentially creates many problems.

While a strong partnership between IT Audit and IT offers many benefits, it is also important for IT Audit to maintain objectivity as a third line of defense. However, the inclusion of an IT audit is not automatic, especially if the IT audit team cannot follow up the IT project. As banks and IT audit departments focus on solving these technology challenges, having the right skills and talent is critical. Both from an IT audit perspective and from a broader IT perspective, resource requirements are changing and banks are challenged to source and manage the resources they need.

One of the biggest challenges for CAEs and IT auditors is the lack of talent with the knowledge and experience to perfect and take a more sophisticated approach to using technology-enabled analysis and auditing. The extent to which automation affects IT auditors may not be known, but automation of exam practice is known. Just as IT auditors need to acquire or sharpen technical skills to keep up with innovations in the banking sector, they also need to contend with innovations in audit practice. It is undoubtedly the lack of skills and talent in IT testing. Banks in all sectors struggle to find the right people. As IT and internal audit functions continue to evolve, they face a growing need to recruit new skills and retrain many existing employees for new skills.

Additionally, with the growing importance of technology in conducting internal audit, the challenge is not in applying technical know-how to legacy projects, but rather in how technology is changing the way the audit is performed. i.e. the risk guarantee. .In addition to identifying the technical skills you need, it is extremely important to recruit talent that also has an entrepreneurial spirit. IT audit functions require professionals who understand the new tools used in audit and across the bank. Because despite the talent and skills we need today, the requirements will likely change in the future as banks change. Therefore, audit skills need to be more fluid. This is an ongoing risk that can arise at any time and requires effective controls to be maintained and updated as necessary. Detailed security assessments are required to account for changes to various processes as a result of large technology projects or other important initiatives. The IT audit must also develop significant recommendations that affect the strengthening of the bank's position in the field of cybersecurity.

Cyber risks have become one of the biggest challenges for companies. A single cybersecurity incident can significantly disrupt operations, result in lost revenue and long-term financial damage, trigger legal and regulatory action, and damage an institution's reputation and customer trust. Of course, these concerns are not limited to the IT audit function. Online criminals are becoming increasingly creative and sophisticated. As banks focus on cybersecurity and protecting their data, they are still lagging behind due to the changing landscape, the increasing sophistication of cybercriminals, evolving regulatory requirements, and persistent loopholes and process flaws created as part of ongoing transformation projects within the bank.

There are significant plans within banks to leverage the transformation, innovation and disruption of new and infrastructure technologies to increase revenue, profitability and shareholder value, as well as productivity and profitability. Already significant investments are expected to increase significantly over the next few years to support IT audits.

Cybersecurity and privacy concerns, as well as broader digital and technology transformations, are prompting another boards to hire tech-savvy executives as new directors and senior advisors. As mentioned above, there is still a severe shortage of qualified IT auditors in the market.

The IT audit function needs to take a new approach to finding the right resources, taking into account both these talent challenges and the evolving needs of the function in the face of changes in their banks.

5.3.Recommendations

The following recommendations are proposed for the challenges of information technology audits in banking sectors;

- IT audit should seek partnership and work together without crossing borders, as they and IT will not always have exactly the same goals or priorities when it comes to strategic technology projects.

- The IT audit function must be prepared and skilled to carry out its audit and assessment responsibilities in a highly efficient and agile manner. This highlights the importance of IT audit adopting a next-generation mindset and implementing the governance, methodologies, and enabling technologies required to support today's highly dynamic, fast-moving banks. This is the future of IT auditing.

- Information technology audit frameworks must stay up-to-date in order to be effective. This means that the framework must be regularly updated according to the latest technological advancements. And must be able to detect potential risks and deficiencies. As technology advances, the risks and deficiencies that are associated with it also change. An effective IT audit framework must be able to detect these changes in order to protect the organization from potential threats. The framework must be able to provide the necessary guidance and assurance to the bank that it is compliant with the latest standards.

- IT audit must be able to access and govern the data being used in order to ensure that various control and compliance requirements are met. Banks must maintain their risk management practices and control structures, placing a significant burden on IT audit functions to keep pace with changes in the bank and ensure that audit plans address these transformations appropriately.

- Banks should begin by investigating the source of their data and establishing clear rules and policies to ensure that it is clean and usable. The ability to leverage advanced technologies in IT audit, in particular, is highly dependent on the quality of data in the bank. Furthermore, as various functions within the bank begin to use these technologies,

- Every day, new cyber threats emerge that threaten a wide range of business systems, and banks face a monumental challenge in keeping up with the threats and protecting their data. It should that cybersecurity is a top priority not only for IT auditors.

- Banks need to adopt a mentality and capabilities oriented toward becoming more data- and technology-enabled Information technology audit function.

References

Begashaw, B. Y. (2018). Factors affecting the quality of Information Technology (IT) audit in Ethiopian commercial banks.

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

Bogale, M. (2016). Auditing IT and IT Governance in Ethiopia. *Semantic Scholar*.

Bogale, M., D. L., & P. E. (2015). Auditing IT and IT Governance in Ethiopia . *ResearchGate*.

Champlain, J. J. (2003). Auditing information systems. . *John Wiley & Sons.*

Davis, Chris, Schiller, & Mike. (2011). IT Auditing: Using Controls to Protect.

Demissie, T. (2018). Assessement of Information System Audit effectiveness: A case study of Commercial Bank of Ethiopia.

guidelines, A. s. (1998).

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

Institute of Internal Auditors (IIA). (2000).

ISACA. (2003). 6th ASOSAI Research Project, IT Audit Guidelines, Research team members Malaysia, India, Australia and China, Septemeber, 2003.

James, A. H. (2005). Information Technology Auditing and Assurance. *Thomson South-Western, USA.*

Jerene, W., & Dr. Dhiraj , S. (2018). The induction of banking technology in Ethiopia: Evidence from public bank. *ResearchGate, 5*(12).

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

Lovaas, P. &. (2012). IT audit challenges for small and medium-sized financial institutions. *Annual symposium on information assurance & secure knowledge management*.

Majdalawieh, M. &. (2009). Paradigm shift in information systems auditing. *Managerial Auditing Journal, 24(4)*, 352-367.

Merhout, J. W. (2008). Information technology auditing: A value-added IT governance partnership between IT management and audit. *Communications of the Association for Information Systems, 23*(1), 26.

Mihret, D. &. (2007). Value-added role of internal audit an Ethiopian case study. *Managerial Auditing Journal, 23(6)*, 567-595.

Moorthy et al. (2011). The impact of information technology on internal auditing. *African Journal of Business Management, 5 (9)*, 3523-3539.

Mr.Avadh Yadav, B. (n.d.). *https://www.bartleby.com/essay/*. Retrieved from Information-Technology-Audit-F3S7RK8KD6VA.

Mr.Avadh Yadav, B. (n.d.). *Information Technology Audit*. Retrieved from bartleby research: https://www.bartleby.com/essay/Information-Technology-Audit-F3S7RK8KD6VA

Ndulu, J. (2004). Survey of the causes of information systems failure among microfinances in Kenya.

No, S. M. (2015-2016). TECH-COMPUTER NETWORKS & SECURITY. *Applicable for students admitted into M. Tech Programs, 3*(2), 163.

Pawan, C. S., & Dr. Jitendra, S. (2019). STUDY OF TECHNOLOGY IN THE BANKING INDUSTRY IN REFERENCE TO BHOPAL. *International Journal of Advance Research and Innovative Ideas in Education, 5*(6), 2395-4396.

Riggins, F. &. (2016). Exploring the impact of information and communication technology (ICT) on intermediation market structure in the microfinance industry. *The African Journal of Information Systems, 8*(3), 1.

Sarens, G. & Abdolmohammadi, M. J. (2011). Monitoring Effects of the Internal Audit Function: Agency Theory versus other Explanatory Variables. *International Journal of Auditing, 15*, 1-20.

Senft, S. &. (2008). Information technology control and audit. *Auerbach publications*.

Siew, E. e. (2017). Factors affecting IT Audit Quality: an Exploratory Study. *School of Business, Monash University Malaysia, Jalan Lagoon Selatan, Bandar Sunway, Petaling Jaya,Selangor, Malasia,,* *2017*.

Siew, E. e. (2017). Factors affecting IT Audit Quality: an Exploratory Study. *School of Business, Monash University Malaysia, Jalan Lagoon Selatan, Bandar Sunway, Petaling Jaya,Selangor, Malasia, Vol. 2017 (2017), Article ID 802423., 2017*.

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

Stoel, D. e. (2012). An Analysis of Attributes that Impact Information Technology Audit. *International Journal of Accounting Information Systems*, 60-79.

US, E. (2019). *Ethiopia - Banking Systems*. Retrieved from www.privacyshield.gov: https://www.privacyshield.gov/article?id=Ethiopia-Banking-Systems

www.searchcompliance.techtarget.com. (2014).

SAINT MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

Research Questionnaire for IT audit staffs

This questionnaire is designed to collect data to assess the practice of information technology auditing in private commercial banks in Ethiopia. The data shall be used for academic purposes only, and it will be treated with the confidentiality it deserves. Your participation in facilitating this study will be highly appreciated.

Kindly tick (√) in the space provided.

With best wishes, thank you very much for your cooperation and time!

Lula Awol Yimam
E-mail: lula.awol@gmail.com
+251911855400

Section I: Background information

Instructions: Please tick (√) from the alternatives that are the most applicable answer to you in respect of each of the following items

1.1. Level of education:

□Diploma level □Bachelor‘s Degree Level

□Masters Level □PHD

1.2. How long have you worked in the banking sector?

□Less than 2 years □2-5 years □6-10 years

□More than 10 years

1.3. What is your overall experience in IT/IS auditing practice?

□Less than 5 years □5 to 10 years □11 to 15 years

□More than 10 years

1.4. Your qualifications

□Accounting and finance □Information technology

□If other, please specify____________________________________

1.5. Certification(if any)

□CIA □CISA □CISSP

□CRISC □If other, please specify________________________

1.6. Current carrier post(position)

□Chief audit executive or equivalent □IT audit director □Audit director

□IT audit manager □IT audit staff

□if other, please specify __________________________

1.7. Have you earned any certificates in your field/ in areas of IT audit after joining the bank?

□If yes, please specify __________________________

□No

SECTION II: Questions related to the practices of information technology auditing

Instructions: Please tick (√) from the alternatives that are the most applicable answer to you in respect of each of the following items

S.no.	Statements	Strongly disagree	Disagree	eutral	Agree	Strongly agree
2.1. Communication with the IT department						
1.	IT auditors collaborate in the strategic technology project of the bank					
2.	A formal process exists to continue or postpone the IT implementation of strategic technology projects if new risks emerge during the implementation process					
3.	Committees/working groups that the IT department invites IT audit to participate in					
4.	The frequency with which the bank's process for identifying and assessing technology risk is carried out					
2.2. IT audit engagement with technology projects						
1.	IT audit have involvement in major technological projects					
2.	In each of the following stages of strategic technology projects, what level of involvement does IT audit have?					
	• Planning					
	• Design					
	• Testing					
	• Implementation					
	• Post implementation					
2.3. Management support						
1.	Your bank’s board of directors engage and understand information risk relating to your business					

S.no.	Statements	Strongly disagree	Disagree	eutral	Agree	Strongly agree
2.	Board of directors (Specifically audit committee) have technical expertise in relation with IT audit					
2.4. Resource, staffing and skills						
1.	Enough IT auditors are available in the bank.					
2.	There are different aspects of your present IT audit plan that you are unable to adequately address due to a lack of resources or expertise.					
3.	IT audits are performed by full-time internal audit professionals in the internal audit department who specialize in IT audit projects.					
4.	There are sufficient numbers of IT auditors available in the market with the required level of expertise to carry out quality audit work.					
5.	Your bank assists you in continuing to learn/train/obtain certificates in your field of expertise/specialization in IT auditing					
6.	The bank facilitates the trainings					
	• In-house trainers					
	• Outside trainers					
2.5. Structure of IT audit						
1.	A designated IT audit manager (or equivalent position) exists in your bank.					
2.	Your bank's IT audit director/manger report:					
	• Chief audit executive					
	• Chief executive officer					
	• Report through some other function					

S.no.	Statements	Strongly disagree	Disagree	eutral	Agree	Strongly agree
	• A director under the CAE					
	• Chief information officer					
3.	IT audit manager (or equivalent position) regularly attends the audit committee meetings.					
4.	The CAE is knowledgeable enough to undertake a discussion with the audit committee about IT audit issues					
5.	The organizational structure of your bank's IT audit resources					
	• Part of the internal audit department not a separate function					
	• Part of the internal audit department but considered to a separate function					
	• Embedded in the bank as a separate audit function					
	• No IT audit resources are available within the bank					
6.	The IT audit is supported with outside resources to supplement or provide your IT skills					
7.	The main reason(s) why your bank hires outside support to supplement IT auditing skills					
	• Lack of resources					
	• In house internal audit department lacks IT audit skill sets different/outside perspectives					
	• Provide the opportunity for people to learn from the experience of outside resources					
	• Variable resource modeling					

S.no.	Statements	Strongly disagree	Disagree	eutral	Agree	Strongly agree
8.	The IT audit hours covered by outside IT audit resource is more compared to the total IT audit hour					
2.6.	**Framework**					
1.	Adequate frameworks are developed to carry out successful IT audit work					
2.	The IT audits framework are developed in accordance with/meets international standards.					
3.	The bank has developed IT risk management framework					
4.	The IT audit risk framework is linked to the bank's IT risk management framework					
2.7.	**IT Security and Privacy/Cybersecurity**					
1.	Recent press coverage on cyberwarfare and/or cybersecurity has affected your interest in and focuses on the subject of information security.					
2.	The board of directors is involved with information security risks relating to the bank.					
3.	The board of directors of the bank is adding technical expertise to the board and disclosure committee.					
4.	Cybersecurity is included in the audit plan.					
5.	Cyber-related audit activities have been performed.					
6.	Cybersecurity audits are typically resourced					
	• Exclusively with in-house (IT audit) resources					
	• In-house resources with support from technical					
	• IT/information security resources					
2.8.	**Data Management and Governance**					
1.	Banks do not devote sufficient attention to how data is collected.					

S.no.	Statements	Strongly disagree	Disagree	eutral	Agree	Strongly agree
2.	Banks look at the source of their data and make sure there are clear rules and policies in place that ensure it is clean and usable.					
3.	IT audit is able to access and govern the data being used to ensure various control and compliance requirements are being met.					
2.9.	**Emerging Technology and Infrastructure Changes — Transformation, Innovation, Disruption**					
1.	Risk management practices and control structures are in place to address emerging technology and infrastructure changes.					
2.	The bank has a long-term strategy to transform IT audit into a data-driven function that makes use of leading technology solutions.					
3.	For banks to receive more efficient audits, deeper insights, and increased risk assurance, a similar level of data and technology enablement is expected within IT audit.					
4.	Data recovery system emplaced.					

Interview Questions for Chief internal Audit Executives

1. Do strategic technology projects involve collaboration with the IT audit function in your bank? What level of involvement does IT auditing have in major technological projects?

2. Does the IT audit plan include cyber security? What cyber-related audit activities have been carried out?

3. Has your bank developed adequate IT audit frameworks that are customized enough to carry out successful audit work?

4. Are there enough IT auditors available in your bank?

5. What is the organizational structure of your bank's IT audit resources?

6. Does the management of the bank render support to the IT audit?

7. How do emerging technology and infrastructure changes challenge or affect an IT audit?

8. Do IT auditors have strong or effective communication with the IT department?

9. Data management and governance with respect to IT audit