



ST. MARY'S UNIVERSITY
SCHOOL OF GRADUATED STUDIES
DEPARTMENT OF ACCOUNTING AND FINANCE

ASSESSMENT OF EDP AUDITING PRACTICES OF ABAY
BANK S.C

BY
BEHAILU BANKSRA

JUNE, 2023

ADDIS ABABA, ETHIOPIA

ST. MARY'S UNIVERSITY
SCHOOL OF GRADUATED STUDIES

ASSESSMENT OF EDP AUDITING PRACTICES OF ABAY BANK S.C

BY
BEHAILU BANKSRA
ID: SGS/0320/2012A

ADVISOR
MOHAMMED SEID (ASS. PROFESSOR)

A THESIS SUMMITTED TO SCHOOL OF GRADUATED STUDIES OF ST.
MARY'S UNIVERSITY IN PARTIAL FULFILLMENT OF THE
REQUIREMENT FOR MBA IN ACCOUNTING AND FINANCE

JUNE, 2023




ADDIS ABABA, ETHIOPIA

ST. MARY'S UNIVERSITY
SCHOOL OF GRADUATED STUDIES

ASSESSMENT OF EDP AUDITING PRACTICES OF ABAY BANK S.C

BY
BEHAILU BANKSRA
ID: SGS/0320/2012A

APPROVED BY BOARD OF EXAMINERS

_____	_____	_____
DEAN, GRADUATE STUDIES	SIGNATURE	DATE
_____		_____
MOHAMMED SEID (ASS.PROF.)	_____	_____
ADVISOR	SIGNATURE	DATE
_____		<u>12/07/2023</u>
ASMAMAW GETIE (ASS.PROF.)	_____	_____
INTERNAL EXAMINER	SIGNATURE	DATE
_____		_____
BIRUK AYALEW (PHD)	_____	<u>14/07/2023</u>
EXTERNAL EXAMINER	SIGNATURE	DATE

DECLARATION

I, Behailu Banksra, declare that this work entitled “**ASSESSMENT OF EDP AUDITING PRACTICES OF ABAY BANK S.C**”, is the outcome of my own effort and study and that all sources of materials used for the study have been duly acknowledged. I have produced it independently except for the guidance and suggestion of my Research Advisor and internal examiner. This study has not been submitted for any degree in this University or any other University. It is offered for the partial fulfillment of the degree of Accounting and Finance.

Declared by;

Candidate’s Name: Behailu Banksra

ID Number: SGS/0320/2012A

Department Name: Accounting and Finance

Course’s Name & Code: Thesis

Student’s Address:

Mobile: 0913-7658-44/ 0909-534-849

Email: behailubanksra@gmail.com

Title of the thesis: Assessment of EDP Auditing practices of Abay Bank S.C

Student’s Signature _____ Date of Submission: June 2023

Confirmation by Advisor

MOHAMMED SEID (ASS. PROFESSOR)



SIGNATURE

DATE

ENDORSEMENT

This thesis has been submitted to St. Mary's university, school of Graduate studies for examination with my approval as a university advisor.

Advisor

St. Mary's, Addis Ababa, Ethiopia

Signature

June, 2023

ACKNOWLEDGEMENTS

First of all Praise be to the Almighty God. My source of success and strength, Next, I am grateful to my families, to this day their help is indescribable. I would like to express my sincere gratitude to my advisor **MOHAMMED SEID (ASS.PROFESSOR)** for his indestructible humility, respect, professional guidance, comments, constructive ideas and advice from the initial to the accomplishment of this study. Thanks a lot to all **ABAY BANK S.C** employees and management staffs for offered to me all necessary information's and filing the questionnaires' that have great contribution for successful accomplishment of this study. I extend my gratitude to my lecturers who taught me in the MSC program, therefore enriching my research with knowledge.

Lastly, I would like express my deepest gratitude to my classmate friends and my friends who been with me since childhood and in my trouble and joys.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	i
LIST OF TABLES.....	v
ABSTRACT.....	vi
CHAPTER ONE.....	1
INRODUCTION.....	1
1.1 Background of the Study.....	1
1.2 Abay Bank Background Overview	2
1.3 Statement of the Problem.....	3
1.4 Research Question.....	5
1.5 Objectives of the Study	5
1.5.1 General Objective	5
1.5.2 Specific Objective.....	5
1.6 Significance of the Study	5
1.7 Scope of the Study.....	6
1.8 Limitations of the Study.....	6
1.9 Organization of the Paper.....	6
CHAPTER TWO	8
LITERATURE REVIEW	8
2.1. Introduction	8
2.2. Theoretical Review	8
2.3. Definition of EDP/IT Auditing	9
2.3.1. The Need for EDP Auditing	10
2.3.2. EDP Auditing Objectives.....	11

2.3.3.	IT Controls	12
2.3.4.	Areas Covered Through EDP Auditing	14
2.3.4.1.	IT Governance	14
2.3.4.2.	Physical Access Control	14
2.3.4.3.	Logical Access Control	14
2.3.4.4.	IT Asset Management.....	15
2.3.4.5.	Disaster Recovery and Business Continuity Plan.....	15
2.3.4.6.	Data Backup and Restoration	15
2.3.4.7.	Data Protection and Privacy	16
2.3.4.8.	IT Application Control	16
2.3.4.9.	Network Security.....	16
2.4.	Challenges Faced in Conducting EDP Audit.....	16
2.5.	Factors Impacting EDP Auditing Effectiveness.....	17
2.5.1.	Auditors It Knowledge and Competency.....	17
2.5.2.	Auditors IT Control Knowledge	19
2.5.3.	Target System Complexity	20
2.5.4.	Auditing Skill.....	21
2.5.5.	Audit Procedure and Methodology.....	22
2.5.6.	Resource Availability.....	23
2.6.	Empirical Literature	24
2.7.	Conceptual Framework	25
CHAPTER THREE		26
RESEARCH METHODOLOGY.....		26
3.1.	Description of the Study Area.....	26

3.2. Research Design.....	26
3.3. Research Approach	26
3.4. Population.....	26
3.5. Sampling.....	27
3.6. Sampling Size Determination.....	27
3.7. Data Collection Method	28
3.8. Questionnaire Design	28
3.9. Methods of Data Analysis	28
3.10. Validity	29
3.11. Ethical Considerations	29
CHAPTER FOUR.....	30
DATA ANALYSIS AND DISCUSSIONS	30
4.1. Introductions.....	30
4.1. Response Rate	30
CHAPTER FIVE	39
SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS.....	39
5.1. Introduction	39
5.2. Summary	39
5.3. Conclusions	40
5.4. Recommendations	41
5.5. Recommendation for Further Researches	42
REFERENCES	43
APPENDIX.....	48

LIST OF TABLES

Table 1: Demographic information of the respondents	31
Table 2: Understand About Auditing Practices	32
Table 3: Challenges of implementing conducting EDP auditing.....	34
Table 4: EDP frauds.....	35
Table 5: EDP auditing fraud detection.....	36

ABSTRACT

The study aims to explore the assessment of EDP auditing practices of ABAY bank S.C, To undertake the study, a descriptive research design was used. The sample consisted of bank employee's managers, credit analysts, supervisors and workers in ABAY bank S.C Addis Ababa hade office. A structured questionnaire was used to collect data from respondents. Random sampling technique was employed to select 205 respondents who have working in ABAY bank S.C direct experience with EDP subject matter. However, 4 respondents did not return the questionnaires and 201 questionnaires were collected. The data obtained from the 201 respondents were analyzed using SPSS version 26 descriptive statistics (frequency, percentage) and inferential statistics like correlation. In doing so, both primary and secondary data employ as a research process to study the various issues involved in the paper. To collect the primary data, Questionnaires, key informant interview and The secondary data were collected from different published and unpublished documents such as relevant theoretical concepts, textbooks, and journal articles, scholarly works and, as well as websites. Based on study finding the conclusion drawn and the researcher recommend that idea for the public to consult and discuss of EDP auditing practices.

CHAPTER ONE

INRODUCTION

1.1 Background of the Study

Electronic data processing (EDP) auditing practice is a critical component of modern auditing, as information technology (IT) systems have become increasingly integrated into organizational operations. EDP auditing is the process of evaluating the effectiveness and efficiency of an organization's IT systems and the controls in place to protect them. This type of auditing is essential for ensuring the accuracy, completeness, and reliability of financial and operational data, as well as for identifying and mitigating IT-related risks (Hall, 2013).

EDP auditing practice involves a variety of techniques and tools, including data analysis, computer-assisted audit techniques (CAATs), and risk assessment methodologies. EDP auditors use these tools to identify potential weaknesses in IT systems and controls, assess their impact on the organization, and develop recommendations for improving them (Hunton, J. E et al, 2019)

One of the primary objectives of EDP auditing is to ensure the integrity of financial reporting. EDP auditors are responsible for verifying the accuracy of financial data and ensuring that it is free from errors, omissions, or intentional misstatements. They also evaluate the effectiveness of internal controls over financial reporting, such as access controls, segregation of duties, and change management procedures, to ensure that they are operating effectively.

In addition to financial reporting, EDP auditing practice also focuses on operational auditing. This involves evaluating the effectiveness of IT systems and controls that support operational processes, such as inventory management, production, and distribution. EDP auditors use data analysis techniques to identify potential inefficiencies, errors, or fraud in these processes and develop recommendations for improving them (Vasant & Sridharan, 2018).

EDP auditing practice is constantly evolving, as new technologies and IT-related risks emerge. EDP auditors must stay up-to-date with the latest developments in the field and continuously adapt their methodologies and techniques to address new challenges. This requires a deep

understanding of IT systems and controls, as well as the ability to think critically and creatively to identify potential risks and develop effective solutions (Hall, 2013).

Finally EDP auditing practice is an essential component of modern auditing, as it helps organizations ensure the integrity of financial and operational data and identify and mitigate IT-related risks EDP auditors use a variety of tools and techniques to evaluate the effectiveness and efficiency of IT systems and controls, and they must stay up-to-date with the latest developments in the field to address new challenges. By doing so, they help organizations operate more effectively, efficiently, and securely (Vasant & Sridharan, 2018).

Recent studies have emphasized the relevance of EDP audit to businesses and have urged further research in this field due to rising investment and reliance on IT for business operations, as well as new regulations and professional requirements connected to the audit of these activities (Stoel, Havelka, & Merhout, 2012).

Researchers explains that in order to protect information system hardware, software, and data from unauthorized access and accidental or deliberate destruction or alteration, as well as to make sure that information systems are operating efficiently and effectively to support the organization in achieving its strategic goals, information system audits evaluate the appropriateness of environmental, physical, logical security, and operational controls (Champlain, 2003). At this juncture, therefore, this study was tries to assess EDP audit practices of Abay Bank S.C, head office.

1.2 Abay Bank Background Overview

Ethiopia's mighty river, the Great Abay, is a dramatic spectacle and a symbol of natural strength and grandeur. It is not only a magnificent sight to visit, but also a river with immense potential for our country's development. This tremendous natural strength similarly explains why we are named Abay. We are here to foster growth and development by promoting and financing different sectors, thereby generating employment opportunities and accelerating capital formation, by ensuring a safe, stable and sound financial system (<https://abaybank.com.et>).

Abay Bank has fulfilled all the necessary requirements of the National Bank of Ethiopia to set up a bank, and officially established on July 14th 2010 and started full-fledged banking operations

on November 3, 2010. Currently, the paid up-capital of the bank is Birr 3.62 billion/ Three Billion Six Hundred Twenty Million Birr until June, 2022, and the number of shareholders reached 4,317/ Four Thousand Three Hundred Seventeen. The Bank is poised to serve all economic sectors through its network of branches. It extends its services to domestic trade and services, international trade, agriculture, industry, transportation, construction and real estate sectors (<https://abaybank.com.et>).

As a number of tourists coming to visit the river Abay watch the impressive scenery and the hospitality of the local people with fascination, our dedicated employees supported by the state-of-the-art banking technology welcome and serve you with diligence and efficiency. Abay River, Ethiopian's jewel, has the potential of being the major catalyst for growth and development of the Country (<https://abaybank.com.et>).

1.3 Statement of the Problem

EDP Auditing Practice, also known as Computer-Assisted Auditing Techniques (CAATs), is a crucial component of modern audit practices. While traditional auditing methods primarily relied on manual processes, EDP auditing practice involves the use of automated tools and techniques to analyze and evaluate large volumes of financial and operational data. However, despite its benefits, EDP auditing practice is not without its challenges and limitations (Arens, A. et al, 2014).

One of the key challenges faced by auditors when implementing EDP auditing practice is the need for specialized technical skills. Auditors must have a strong understanding of computer systems, data structures, and programming languages to effectively use EDP auditing tools and techniques. Additionally, the rapid pace of technological change means that auditors must continually update their skills to keep pace with new developments in EDP auditing practice (Cascarino, 2017).

Many firms face challenge due to auditors is the need for data quality and integrity. EDP auditing tools rely on accurate and complete data to generate accurate results. However, poor data quality, data errors, and incomplete data can lead to inaccurate audit findings and conclusions. Therefore, auditors must have robust data validation and verification procedures in

place to ensure that the data used in EDP auditing practice is accurate and reliable (Hunt, Bryant & Bagranoff, 2004).

Furthermore, auditors must also ensure that they maintain the security and confidentiality of the data they use in EDP auditing practice. Given the sensitive nature of financial and operational data, auditors must have appropriate access controls and data protection measures in place to prevent unauthorized access or misuse of the data (Arens, A. et al, 2014).

Another challenge that auditors face in implementing EDP auditing practice is the need for effective communication and collaboration with IT departments and other stakeholders. Auditors must work closely with IT departments to obtain access to the necessary data and systems, and to ensure that the EDP auditing tools and techniques are effectively integrated into the organization's IT infrastructure (Arens, A. et al, 2014).

The interaction of four factors system audit quality, management support, organizational context, and qualities of the audited is likely what determines how well an internal audit office fulfills its purpose. Achieving audit effectiveness requires management commitment and resource support for the internal audit recommendations. Additionally, the organizational environment in which internal audit occurs, including the office's organizational status, internal structure, and rules and procedures that apply to each auditee, should facilitate efficient audits that result in valuable audit results. Additionally, the success of audits is impacted by the auditee's abilities, attitudes, and amount of cooperation (Mihret & Yismaw, 2007).

According to the researcher bird review, previous studies Especially Berhanu Balcha (2018), Kantilal Chandmal Jain (1968), Erick Anthony (2015), Bzuwerk Yemer (2018) and Tigist Alemayehu (2021) have a conceptual gap because the concepts of electronic data process auditing have not been discussed in depth and various multidisciplinary reading approaches were lifted, methodological, conceptual and majority studies due attentions on effective auditing on financial performance.

This study tries to fill the research gap by focusing to assessing electronic data processing (EDP) Auditing practice of Abay bank SC, head office.

1.4 Research Question

1. What are the key factors that influence the EDP auditing practice in the Abay Bank S.C.
2. What are the challenges faced in practicing EDP audit assignment?
3. What is EDP audit fraud detection approach against EDP fraud?

1.5 Objectives of the Study

1.5.1 General Objective

The general objective of the thesis is to assess of EDP Auditing practices of Abay bank SC.

1.5.2 Specific Objective

The study undertaken to address the following objectives:

- To analyzing the factors that influence the EDP auditing practice in the Abay Bank S.C.
- To identify the challenges faced in practicing EDP audit in Abay Bank S.C.
- To assess EDP audit fraud detection approach.

1.6 Significance of the Study

The substantial purpose of the study will be to examine EDP Auditing practice of Abay bank. Subsequently, the finding of this study improves to the stock of knowledge on the area of EDP Auditing practice in the banking industry. Specifically, this study is significant in the understanding that it helps managers and other stake holders in Abay bank and other banking firms to determine their position and take necessary actions to improve their performance in terms of EDP Auditing and make a better informed decision and The findings of the study will provide relevant input to policy makers. Additionally, it may also provide a support or potential reference to other researchers who are interested to conduct further study on similar areas and it will enable the researcher to acquire good practice and to fulfill preconditions for graduation.

1.7 Scope of the Study

The scope of the study is limit itself to surveying, interviewing and documentary analysis to analyzing EDP audit practice and challenges of Abay Bank S.C., so this study was limit to the case of Abay Bank S.C Head Office only because the geographical samples will obtained from Head Office, the thematic area of the study related with the EDP audit practice and challenges. Second, Based on the total population size the study was random sampling procedure and the study is going to be limited on time because it was be conducted.

1.8 Limitations of the Study

This study did not come to an end without problems, the main influences that donated to the limitation of the study.

First in data collection, some respondents were Abay Bank S.C. head quarter to obtained information. Specifically, these studies confined in head office so due to this case some respondents were not punctual in returning the questionnaire and were not interested to fill questionnaire. And also, this study used a mixed method, which includes together qualitative and quantitative approaches to entertain the research questions.

1.9 Organization of the Paper

This paper was organized in to five chapters. The first chapter dealt with the introductory part of the study. Which includes background of the study, significance of the study, statement of the problem, objectives of the study, scope and limitation of the study, operational definition and organization of the paper are incorporated.

The second chapter would be a brief literature review regarding with research topic. The research methodology and design were discussed in the third chapter. Chapter three discusses the research methodology including, research design, area of the study, research approach, Sampling Design and procedure, method of data collection, data collection methodology, method of data analysis, validity, reliability and ethical consideration. Chapter four data analysis and presentations highlights obtained data from the respondents.

Research findings, results, remarking conclusion and proposed recommendations were presented in Chapter five. The questionnaire and the interviews that were used for data collection were attached to this document as an appendix.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

In this chapter, literatures related to Privatization and liberalization was review. It is organized into different sub topics: definition of EDP auditing, need of EDP auditing, EDP auditing objectives, areas Covered through EDP Auditing, empirical literature review and conceptual framework was briefly discussed.

2.2. Theoretical Review

The majority of businesses, whether for-profit or nonprofit, private or public, are becoming more and more reliant on information technology, which has also had a significant impact on the business environment in three other ways: IT has increased the ability to store, capture, analyze, and process enormous amounts of data; IT has significantly impacted the control process; and IT has also had an impact on the auditing profession in terms of the skills and knowledge needed to conduct an audit (Nurmazilah & Farida, 2011).

Information technology is becoming increasingly important, and there is a need to manage IT-related risks and get more value from IT expenditures. Business leaders and managers are taking charge and implementing organizational changes to build a more efficient framework for managing and keeping track of IT-related objectives and problems. IT auditors should be very knowledgeable about IT risk and controls to give management assurance (Amoroso, Bogale & Kinfu, 2015).

The audit profession has also been significantly impacted by the widespread use of IT in business today. One of the main issues confronting assess the practice of EDP audit fraud detection approach against EDP related frauds the audit profession is keeping up with new technology and ensuring that it operates in a secure and regulated environment (Komnenić, 2009)

Additionally, risk considerations specific to accounting, audits, and systems are presented by IT. That is, the entity's systems, business operations, and financial/accounting activities are all in

danger due to IT. That danger is exclusive to IT, and it would not exist at least not to the same degree-without IT. The inherent risk connected with IT must be identified and evaluated by an expert, such as an IT auditor. Systems-related problems, such as system development, change management, and vulnerabilities, as well as other technology-specific elements, are some of these risk factors (Singleton, 2014).

IT auditing, formerly known as Electronic Data Process (EDP) Auditing, evolved to primarily as a result of the advancement of accounting system technology, the requirement for IT control, and the effect of computers on the capacity to provide assurance services. Compared to auditing as a whole, IT auditing has a brief but rich history and is still a discipline that is constantly developing (Nkwe, 2011).

To guarantee that information systems and related activities are running as intended, IT auditors assess the effectiveness and efficiency of IT controls in those systems and related operations (ISACA, 2010). The IT audit activity offers assurance regarding crucial hazards, particularly those brought about or made possible by the adoption of IT. Information technology auditing has therefore expanded quickly as a result of the rising reliance of corporate operations on IT and new requirements addressing the assurance of IT for such activities (Stoel et al., 2012).

2.3. Definition of EDP/IT Auditing

EDP auditing, also known as computer-assisted auditing techniques (CAATs), is a crucial component of modern audit practices. EDP auditing involves the use of automated tools and techniques to analyze and evaluate large volumes of financial and operational data. The use of EDP auditing techniques and tools has become increasingly important in recent years, as organizations have become more reliant on technology to manage their financial and operational processes (Alles & Kogan, 2013).

EDP auditing is its ability to improve the efficiency and effectiveness of the audit process. EDP auditing tools can analyze vast amounts of data quickly and accurately, allowing auditors to identify potential risks and issues more efficiently than traditional audit methods. Additionally, EDP auditing tools can be used to automate routine audit tasks, freeing up auditors' time to focus on more complex and high-risk areas (Cascarino, 2017).

EDP auditing techniques and tools is not without its challenges. One of the key challenges faced by auditors is the need for specialized technical skills. Auditors must have a strong understanding of computer systems, data structures, and programming languages to effectively use EDP auditing tools and techniques. Additionally, the rapid pace of technological change means that auditors must continually update their skills to keep pace with new developments in EDP auditing practice (Hunton, J. E et al, 2004).

EDP auditing tools rely on accurate and complete data to generate accurate results. However, poor data quality, data errors, and incomplete data can lead to inaccurate audit findings and conclusions. Therefore, auditors must have robust data validation and verification procedures in place to ensure that the data used in EDP auditing practice is accurate and reliable. Ibid

2.3.1. The Need for EDP Auditing

Computers are essential for helping an organization process data and make decisions, but their use must be managed because of how quickly technology is changing and how much money is occasionally invested in them (Amoroso, Bogale, & Kinfu, 2015). Additionally, the costs associated with errors and irregularities that occur in these systems can be significant. Not only must their usage be controlled, but also the manner in which they are used and their effect on the overall goals of an organization must be assessed (Abera, 2020). This calls for the auditor's involvement in supporting and assisting with the implementation of corporate governance in IT and management (Amoroso, Bogale, & Kinfu, 2015). Due to accounting scandals and greater regulation in recent years, there has been a significant growth in the need for IT audits. Information systems are made more secure, dependable, and accurate through IT auditing. According to ISACA, an IT auditor can assist businesses with implementing control structure procedures such as Control Objectives for Information and Related Technology (COBIT), the Committee of Sponsoring Organizations of the Tread-way Commission (COSO), and International Organization for Standardization (ISO) standards 9000, 9001, 17799, and their updates (Walker, 2015).

Due to their guarantee of the accuracy, dependability, and quality of the information generated by the business's information systems, IT audits are crucial organizational activities that offer value to the organization (Siew et al., 2017). An IT audit is required to ensure that the data

collected through systems is functional, secure, and under control. According to Björklund and Joelsson (2015), the IT auditor's contribution to risk management and response within organizations is becoming increasingly significant.

Additionally, companies require reassurance that the internal controls controlling business computer/system operations are sufficient due to the growing reliance on computers for daily tasks and the enhanced threats and hazards associated with new technology (Harb, 2012).

All businesses should do an IT audit, but it is crucial for banks and financial institutions to do so since they are legally compelled to do so in order to sustain their IT infrastructure, safeguard non-public client information, and carry out an annual risk-based audit (Lovaas and Wanger, 2012). An IT audit offers more dependable and accurate information on maintaining data integrity and protecting IT assets. The ultimate result of an IT audit consists of more than just a report; it also includes impacts and the prompt execution of suggestions and remedial actions (added value) with the aim of achieving all of the company's business objectives (Rotim & Komneni, 2010).

2.3.2. EDP Auditing Objectives

IT auditing is done to see whether an information system is meeting its stated organizational goals and to make sure it is not putting the company at an unacceptably high risk (Rahman, 2014). Additionally, an IT audit makes sure that IT resources support company objectives and maximize resource use (Panwar et al., 2014). Additionally, the goal of an IT audit is to identify areas for improvement and confirm that the business is in compliance with all applicable rules and regulations are both internally and externally imposed (Lovaas and Wanger, 2012).

The goal of an IT audit is to assess a company's computerized information system in order to determine whether it generates timely, accurate, complete, and reliable information outputs, as well as to ensure data confidentiality, integrity, availability, and reliability and compliance with applicable legal and regulatory requirements (Lovaas & Wagner, 2012).

Confidentiality: refers to "the safeguarding against unlawful exposure of sensitive information." If information confidentiality breaches potentially cause serious harm to the organization's

reputation among the public, management requires assurance of the organization's capacity to safeguard information confidentiality.

Integrity: This relates to the "accuracy, completeness, and validity of information with respect to company values and expectations. It gives management reassurance that they can rely on and have faith in the information generated by the organization's information systems to make business choices.

Availability: The availability of information as required by the business process now and in the future, as well as the protection of critical resources and related skills, it ensures that they will have access to the data they need to make decisions when necessary.

Reliability: refers to "the degree of consistency of a system or the capacity of a system to execute its needed function under defined conditions. The assurance that the system continuously functions and carries out its stated function as intended is provided by the IT audit.'

Compliance with Legal and Regulatory Requirements: "Compliance deals with complying with those laws, regulations, and contractual obligations to which the business process is subject."

2.3.3. IT Controls

Control goals relating to information security needs are met through IT controls. The central goals, often known as C-I-A, Confidentiality: prevents unauthorized individuals from reading sensitive information such as financial data and credit card numbers. Integrity: Preserves the integrity of vital IT resources, such as hardware, software, and data storage systems. Makes certain that essential IT resources, including hardware, software, and data, are accessible when needed (Wood, Brown & Howe, 2013).

Risk management, adherence to internal policies and guidelines as well as external laws and regulations, periodic and ad hoc management reports, progress checks, and plan revisions are all examples of internal controls. They also include audits, assessments, and monitoring (Panwar et al., 2014). The organizational structures, rules, and practices that are used to secure an organization's assets, maintain the integrity and dependability of its records, and ensure operational compliance with management standards are reflected in the controls of a computer

information system (Panwar et al., 2014). IT controls provide assurance about the dependability of information and information services and are used to help reduce the risks associated with a company's use of technology (Coderre & Police, 2005). General IT Controls and Application IT Controls are two kinds of IT controls that are used to reduce risks connected to the IT environment and application systems (Panwar et al., 2014).

IT General controls, which are concerned with the general environment in which the IT systems are designed, operated, managed, and maintained, form the basis of the IT control framework. All these have as their primary emphasis the administration and monitoring of the IT environment, which has an impact on all applications. For a certain organization or systems environment, general IT controls are applied to all system parts, functions, and data. These measures are intended to assure the proper design and execution of programs, the integrity of program and data files, and the reliability of computer operations (Panwar et al., 2014). According to Panwar et al. (2014), the most prevalent controls include logical access controls over infrastructure, applications, and data; controls for the system development life cycle; controls for program change management; physical security controls over the data center; controls for system and data backup and recovery; and controls for computer operation (Coderre & Police, 2005).

IT controls for applications are specialized controls that are particular to each application system. They consist of maintenance and other forms of data entry; data encryption for transmission; processing controls; and controls that serve to assure correct authorization, completeness, accuracy, and validity of transactions, among other things. According to Panwar et al. (2014), these controls are used to give assurance (mainly to management) that all transactions are genuine, approved, and documented (Coderre & Police, 2005). Application controls' main goal is to make sure that input data is accurate, complete, authorized, and correct; that data is processed as intended within a reasonable amount of time; that data is stored accurately and completely; that output data is accurately and completely; and that records are kept to track the data's progress from input to storage and finally to the final output (Bellino, 2016).

2.3.4. Areas Covered Through EDP Auditing

2.3.4.1. IT Governance

IT governance is the overarching framework for IT operations and a crucial component of enterprise governance in an organization to make sure that IT investment and activities are in line with and satisfy the company's goals (Panwar et al., 2014).

The objectives of IT governance are that IT is aligned with the company, IT enables the business and optimizes benefits, IT resources are utilized properly, and IT risks are handled effectively. The main instrument for IT governance is IT auditing, and IT auditors are involved in providing confirmation that each of these goals has been achieved. Employees with business and IT abilities are required for simple IT auditing implementation (Nkwe, 2011).

2.3.4.2. Physical Access Control

Physical access control refers to limiting access to a specific physical area within a company or organization. This kind of access control restricts access to spaces, structures, and tangible IT assets. Physical access control also keeps track of who enters and exits restricted locations.

Physical and environmental controls aim to shield IT services from intrusion and illegal access. Computer hardware and the data they manage and store should be shielded from unauthorized users in order to achieve this goal. Additionally, they need to be shielded against environmental hazards like fire, water damage (from real flooding or excessive humidity), earthquakes, electrical power surges, and power outages. The organization's IT security policy should take environmental and physical threats into account (Hall, 2011).

2.3.4.3. Logical Access Control

Logical access controls are those that, when a user's identification has been verified, either block or permit access to resources. When a user logs in, they should only have access to the resources they need to do their jobs (Vacca, 2013).

Logical access controls are meant to prevent unauthorized access to, modification of, or deletion of the programs and underlying data files. The goals of access control are to make sure that:

users have only the access necessary to carry out their responsibilities; access to extremely sensitive resources, such as security software programs, is restricted to a small number of people; and employees are prohibited from carrying out incompatible tasks or tasks that are outside the scope of their duties (Hall, 2011).

2.3.4.4. IT Asset Management

IT asset management (ITAM) refers to procedures and plans for monitoring, controlling, and improving privately held IT infrastructure, including software, hardware, operations, and data. IT departments deploy, track, and manage IT assets as part of an ITAM strategy, and determine if those assets need to be optimized, replaced with a less expensive choice, or upgraded to a newer technology (White, 2019). The goals of IT asset management are to provide the company with a thorough understanding of its information systems so that it may use this knowledge for issue detection and swift problem-solving (White, 2019).

2.3.4.5. Disaster Recovery and Business Continuity Plan

Plans for IT disaster recovery include detailed instructions for restoring interrupted systems and networks and assisting in their return to regular functioning. These procedures aim to reduce any detrimental effects on business operations. The processes required to restart, reconfigure, and restore important IT systems and networks are defined by the IT disaster recovery process, which also prioritizes their recovery time target. Additionally, a thorough IT DR strategy contains all the necessary supplier connections, sources of knowledge for restoring interrupted systems, and a logical flow of actions to be taken for a seamless recovery (Hall, 2011). Limiting risk and returning an organization to its pre-incident state as quickly as feasible are the goals of a DR and BC plan.

2.3.4.6. Data Backup and Restoration

In the event that the original data and applications are lost or damaged as a result of a power outage, cyber-attack, human error, disaster, or some other unforeseen event, backup and restore refers to technologies and practices for periodically making copies of the data and applications to a different, secondary device and then using those copies to recover the data and applications and the business operations on which they depend. The goal of the data backup is to produce a copy

of the data that can be retrieved in the case of the main data failure. Data corruption, hardware or software failures, human error, such as a hostile attack (malware or virus), or unintentional data erasure (ISACA, 2010) are all examples of primary data failures.

2.3.4.7. Data Protection and Privacy

The area of information technology (IT) that deals with an organization's or person's capacity to decide what data in a computer system can be shared with third parties is known as data privacy, also known as information privacy (Rouse, 2016). Data protection and privacy are intended to safeguard the "rights and freedoms" of living people and to guarantee that their personal information is not handled without their knowledge and, where feasible, with their agreement (Alemayehu, 2021).

2.3.4.8. IT Application Control

Application controls are specific to an application and may have an immediate effect on how particular transactions are processed. These measures are taken to ensure that every transaction is legitimate, approved, completed, and recorded. The goals of IT application controls are to guarantee the validity of entries made to each record as a result of program processing, as well as the completeness and correctness of records (Hall, 2011).

2.3.4.9. Network Security

A network administrator's rules and procedures for preventing and monitoring illegal access, system modification, abuse, and denial of a computer network and network-accessible resources make up network security. Network security's primary goal is to protect the confidentiality, integrity, and availability of networks and data (Anchugam & Thangadurai, 2018).

2.4. Challenges Faced in Conducting EDP Audit

Finding and documenting highly technical findings is frequently a part of an IT audit. Effective IT audits demand this level of technical sophistication. Likewise, it's important to convert audit findings into business consequences and vulnerabilities that operational managers and senior management can understand. Budget restrictions are frequently highlighted as a key barrier to the implementation of successful and thorough IT audits in many developing nations. Due to the

same factors that limit the degree of IT deployment as a whole, there are also fewer applications for subsequent audits that verify the integrity of the IT systems (Senft & Gallegos, 2008). However, technological development has resulted in an explosion of new dangers to IT-based systems, necessitating ongoing testing against the most recent standards and comparisons of the IT systems to international standards (Hall, 2011).

Limited implementation of these tools in IT audits is caused by low expertise in using IT auditing tools among IT auditors. For the best usage of certain of the packages, such as sequence query languages, knowledgeable programmers are required. Effective IT auditing is greatly hampered by the conventional auditors' lack of availability of these abilities (Champlain, 2012).

The insufficiency of controls in developed apps is a significant problem for IT auditing. Although the application development process should provide for the necessary degree of security, many firms frequently produce apps that stray from the standard application development process and are not fully tested, making them lacking in many areas that IT audits look at (Ndulu, 2004).

IT auditing includes an essential section on disaster recovery and business continuity. Disaster recovery planning is often more of a theory than a reality in enterprises. When a disaster occurs, there is typically very little business continuity since several DR planning components have not been adequately tested and there hasn't been any disaster simulation (Ndulu, 2004). IT security is crucial and should be taken into account while conducting an explicit IT security audit. There are several components to information security, the majority of which are highly technical and require specific abilities not frequently present within the audit teams of many firms. This is a clear difficulty encountered in IT audits in many underdeveloped nations (Ndulu, 2004).

2.5. Factors Impacting EDP Auditing Effectiveness

2.5.1. Auditors It Knowledge and Competency

This study identified one of the independent factors as the IT knowledge and proficiency of the auditors. According to Carroll et al. (2009), an IT audit is performed by auditors who utilize their technical expertise to examine computer systems or offer auditing services when procedures, data, or both are integrated into technology (Carroll et al., 2009). It became more-clear that the

auditing profession needed to modernize as more and more accounting and business processes were computerized. As the systems being audited used technology more often, new methods of assessing them were necessary (Hall, 2004).

According to Komnencic (2009), the IT auditor must have the required professional and technical proficiency to cover the audit's scope. An IT auditor should be capable of comprehending technical regulatory knowledge, auditing techniques, and interpersonal and communication skills. Basic education, a variety of abilities, extensive training, and, of course, certifications are all crucial for an IT auditor. The importance of multidisciplinary education and specialties is rising in the field of IT auditing (Komnencic, 2009).

Due to the ICT industry's fast development and change, IT auditors must maintain a continual level of expertise and technical understanding. IT auditors must also have talents, skills, and education in multidisciplinary disciplines. Furthermore, certification in the CIA, CISA, CISM, or another professional education program is crucial for the IT audit profession (Komnencic, 2009).

Prior research has shown that IT auditors need to have knowledge and expertise in IT-specific knowledge in order to be able to identify material flaws in IT systems. It has been demonstrated that those with specialized IT professional credentials and certificates are more likely to be involved in auditing IT governance, risks, and controls. IT and accounting system knowledge has been shown to be critical to the quality of IT audits (Stoel et al., 2012). Additionally, it takes specific knowledge and experience to examine infrastructure, including networks, routers, firewalls, wireless devices, and mobile devices (Richard, 2005). Additionally, IT auditors need to be knowledgeable about the tools and procedures that will enable them to audit "through the computer" rather than "around the computer" (Siew et al., 2017).

According to Carroll et al. (2009), auditing professions need to be incorporated into a new, developing, unbiased profession that draws on the knowledge, skills, competence, and experience of both audit and IT professionals due to the rising usage of information systems by most enterprises. Additionally, they claim that an IT audit is related to auditors that utilize technical expertise and knowledge to audit through computer systems, offer audit services where data processes are incorporated in technologies, or both (Carroll et al., 2009).

Internal auditors concentrate on testing IT controls and procedures that mitigate known business risks. Additionally, the problems of participating in the organization and planning of IT projects, the implementation of suggested solutions, the supply and support of IS, and the monitoring of the procedures, controls, assurance, and assessment present themselves to IT auditors (Carroll et al., 2009). Therefore, in order to succeed, IT auditors must engage in studying and acquiring knowledge of both IT and auditing.

According to Siew et al. (2017), IT audit quality is substantially connected to IT knowledge and competencies. They recommended placing a focus on teaching and training the audit team members to ensure that they have the necessary IT knowledge and skills to increase audit quality. People with IT experience therefore have the benefit of being able to detect risks and controls within IT knowledge areas as well as grasp more technical and IT concepts (Siew et al., 2017).

2.5.2. Auditors IT Control Knowledge

One of the independent factors in this study has been identified as Auditors' IT control knowledge. IT is a dynamic environment that encourages organizational and process transformation. As a result, fresh threats surface often. Controls are therefore necessary to offer ongoing proof of their efficacy, and this proof must be regularly monitored and analyzed. IT controls assist in reducing risks connected to a company's use of technology by providing assurance regarding the dependability of information and information services. IT controls include: Corporate policies to their physical implementation within coded instructions; Physical access protection through the ability to trace actions and transactions to responsible individuals; and Automatic edits to reasonability analyses for large bodies of data (Richard, 2005).

The assurance of the internal IT auditor is a neutral and unbiased evaluation of whether the IT-related controls are working as planned. Understanding, investigating, and evaluating the important controls in relation to the risks they manage, as well as carrying out enough testing to make sure the controls are suitably designed and operating successfully and constantly, are the foundations of this assurance (Richard, 2005). IT internal auditors should be able to evaluate the internal audit methods and structure of a company for IT risk and control, compliance, and assurance. Internal auditors are required to review and evaluate the risks and controls for information systems that are used by the company, according to the International Institute of

Internal Auditors' (IIA), International Standards for the Professional Practice of Internal Auditing. Standards are principle-focused and provide a framework for performing and promoting internal auditing. The Standards are mandatory requirements consisting of: Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance (Richard, 2005). Internal auditors need to understand the range of controls available for mitigating IT risks. In their study, Alraja and Alomiam (2013) discovered a substantial connection between general controls of information systems auditing and information systems performance, as well as a considerable influence of general controls of information systems auditing on information systems performance (Alraja and Alomiam, 2013). In light of this, the researcher utilized the characteristics for the IT control knowledge factor from the survey literature, such as knowledge of IT governance, general IT controls, including knowledge of information security, and application controls (input, process, and output controls) (Siew et al., 2017).

2.5.3. Target System Complexity

Target System Complexity was found as one of the independent factors in this study. This element, according to Siew et al. (2017), relates to how challenging it is to audit the auditee. According to their literature, this construct depends on the auditee's company size and scale, the audit's breadth, the auditee's cooperation, and the dependability of the internal controls. They added "Business Scale and Audit Scope" and "Auditability" for this element to the goal of system complexity. The number of geographically scattered business units, the quantity of involved business units, processes, or systems, the auditee's support, and the degree to which the internal control is specified and documented are all indicators of their existence (Siew et al., 2017).

The process or system category, which Merhout and Havelka (2007) defined in their research as including any criteria depending on the process or system being audited, i.e., the audit's aim, and unique considerations for the particular audit "project" being undertaken, Clear project scope, system complexity and kind, the quantity of manual work against automation, and the degree of documentation for the process or system are a few examples of processing system factors (Havelka and Merhout, 2007).

2.5.4. Auditing Skill

One of the independent factors in this study that has been found is auditing expertise. IT auditors must have a technical grasp of information systems and an understanding of the controls required to guarantee the correctness, validity, timeliness, and completeness of organizational information, resources, and assets. Because of this, the combination of IT and auditing experts' knowledge, abilities, experience, and day-to-day duties and responsibilities is categorized as IT auditing. As a result, individuals with diverse backgrounds (in IT and/or auditing) are compelled to acquire the skills essential to succeed in the field of IT auditing (Carroll et al., 2009). Because IT auditing is so reliant on IT and in order to bridge the gap between the IT and auditing fields, an IT auditor must be knowledgeable in both IT and auditing.

A variety of specialized sub-skills that go under the category of auditing include creating and carrying out an audit plan, creating and using checklists, following up, recording results, etc. Communication and interpersonal skills are also crucial for the IT audit role since they increase the likelihood that the audit will be successful if the auditors can connect and communicate effectively with all parties. A genuine regard for people, active listening (ensuring you comprehend what is being said), spending three times as much time listening as talking, and oral and written communication abilities, among other qualities, are some examples of strong interpersonal and communication skills for internal auditors (Komnenic, 2009).

For example, to help clarify the statement that audit knowledge should be applied to IT knowledge, an audit knowledge concept, "understanding of the concept of risk," should be applied to a specific area of IT knowledge depending on the scope and objective of the audit. Carroll et al. (2009) described how audit knowledge should be applied to IT knowledge to enable an IT auditor to execute his or her daily roles and responsibilities (Carroll et al., 2009). The notion of gathering and analyzing pertinent audit evidence was also a necessary component of auditing competence.

According to Stoel et al. (2012), accounting knowledge and audit skills are the second-most frugal components. This element is referred to as the audit personnel's expertise in accounting and auditing in general; their understanding of the accounting system being audited in particular; and their capacity to carry out tasks and use professional judgment as auditors. They said that

previous studies, mainly in the field of financial audit research, have explored the effect of audit employee knowledge and competence on audit quality (Stoel et al., 2012).

Due to their understanding of auditing principles and ability to recognize how risks affect financial statements, people with auditing backgrounds have an advantage given the logic of applying IT expertise to audit knowledge. As a result, the researcher used the survey literature's attributes for the auditing skill factor, such as knowledge of the concept of risk, familiarity with relevant standards and best practices, knowledge of the business process, ability to obtain and interpret pertinent audit evidence, communication ability, and independence (Carrol et al., 2009 and Havelka and Merhout, 2012).

2.5.5. Audit Procedure and Methodology

A well-planned, properly designed audit program is crucial in order to assess risk management procedures, internal control frameworks, and adherence to corporate policies with regard to IT-related risks at institutions of every size and complexity. Effective audit programs emphasize risk, encourage solid IT controls, guarantee that audit flaws are promptly corrected, and notify the board of directors of the efficiency of risk management procedures (Lovaas, 2009).

Yeghaneh et al. (2015) discovered that having an appropriate framework, audit processes, methodologies, forms, and other tools may help auditors execute high-quality audit work and impact the quality of IT audits (Yeghaneh et al., 2015).

According to Merhout and Havelka (2007), the audit process or methodology factor relates to the particular steps and methods that the IT audit team takes. The availability of an audit methodology for the team to follow, coordination between the financial and IT auditors, the implementation of effective project management techniques, and the assessment of field work by a supervisor or senior staff member are some of the components found (Merhout and Havelka, 2007). The use of suitable templates forms or other tools by the audit team to perform the audit as well as the right documentation and sign-off processes for each stage of the audit were determined to be the fifth most frugal element by Stoel et al. (2012).

In light of this, the researcher used the characteristics of the audit procedures and methodology factor from the survey literature, such as the existence of an audit methodology for the team to

follow, scope definition, the use of automated tools, and timely oversight and review of audit work. Additionally, the audit team makes use of standard forms and templates for documentation, and the audit team has strict sign-off procedures for completed audit steps (Merhout and Havelka, 2007 and 2008; Stoel et al., 2012; and Yeghaneh et al., 2015).

2.5.6. Resource Availability

Resources include the time, money, and audit employees that the audit team could access to support their IT auditing tasks (Stoel et al., 2012). According to Siew et al.'s research, resource availability includes factors like whether computer-assisted auditing tools (CAATs) are used, whether there is sufficient time to conduct the IT audit, whether there is sufficient funding available to conduct the IT audit, and whether there is sufficient staff to carry out the IT audit in a way that is appropriate (Siew et al., 2017).

Merhout and Havelka (2007) discovered that the features of the organization's IT audit function are included in the IT audit organization category. The scale of the IT audit organization in relation to the entire business, the leadership of the IT audit unit, the availability of funds and resources, and the usage of technology for testing are a few examples of these characteristics (Merhout and Havelka, 2007). In their study, Yeghaneh et al. (2015) looked at and advised that having an accurate budget is necessary before performing any audit task. Additionally, they have recommended that in order to do high-quality audit work, auditors accept and carry out the audit while taking into account the availability and access to credible resources (Yeghaneh et al., 2015). According to Stoel et al. (2012)'s study, planning and methodology, resource availability, and auditee relationship are elements that are special to the individual audit engagement and must be taken into account as part of IT audit quality.

As a result, the researcher utilized the attributes for the Audit Procedures and Methodology factor from the survey literature, including whether computer-assisted auditing tools (CAATs) are used, whether there is sufficient time to conduct the IT audit, whether there is sufficient funding available to conduct the IT audit, and whether there is sufficient staff to properly conduct the IT audit (Stoel et al., 2012; Yeghaneh et al., 2015; Siewa et al., 2017).

Giving IT audit and assurance professionals more abilities to evaluate both the business and technical aspects of a problem would benefit both the enterprise and the professional in terms of

the quality and relevance of the analyses performed and the recommendations made (Robert, 2010).

2.6. Empirical Literature

Empirical literature review is commonly referred to as a systematic literary review. In particular, it examines previous research studies. It gives due summaries of previous studies of similar content. The purpose of the Empirical review is to identify gaps in a literature and to direct the study in comparison with previous research. The Empirical review is foundation stone used to establish the theoretical basis of the study. This part was summarizing the empirical review of EDP auditing practices.

(Berhanu, 2018, "assessment of performance audit practice: the case of Ethiopian public sector enterprises")

Efficient, effective & economical use of once own scarce resources should be the foremost objective of a given country so as to ensure its all rounded growth. Those organizations (corporations) that haven't started to do pa should start doing it without taking considerable time. Meanwhile, the management bodies of such organizations should give proper attentions to this discipline like that of financial as well as compliance audits. Moreover, the preparations of pa manuals/ standards in the PS organizations, where there is/ are not, should be facilitated.

(Bzuwerk, 2018 conducted study on factors affecting it audit quality in commercial banks in Ethiopia), the general approach of this research was an exploratory study in which a combination of quantitative and qualitative methods has been used to collect and analyze data.

(Tariku, 2018, conducted study on assessment of information system audit in case of commercial bank of Ethiopia), factors such as career and advancement, professional competence, quality of audit work, professional competency relationship between internal and external auditor and top management support.

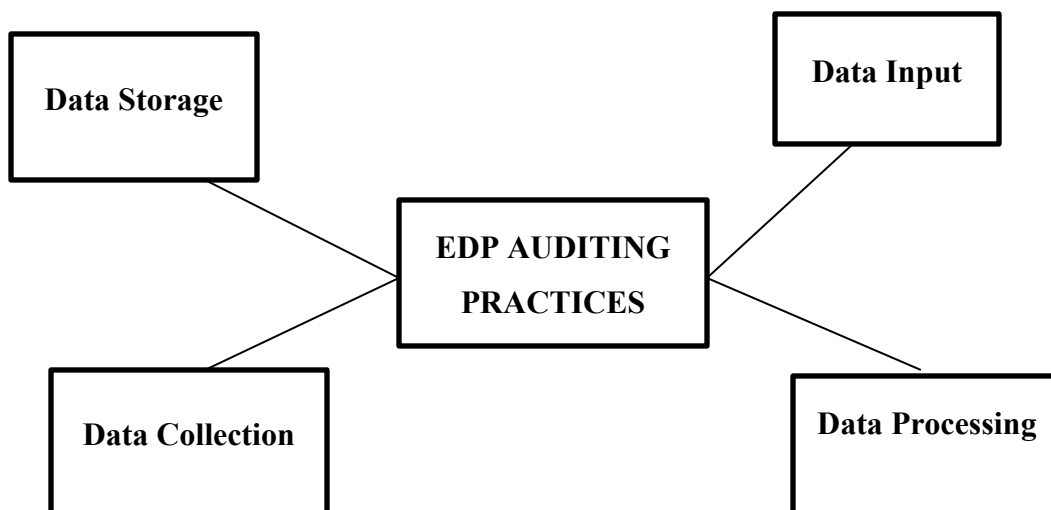
(Julia, 2013 conducted study on the it audit and fraud detection in commercial banks of Kenya), study focused on commercial banks in Kenya. The study tries to find to determine the extent of it related fraud in Kenyan commercial banks, to establish the challenges faced during it auditing by the is auditor, to establish the countermeasures implemented in preventing fraud through it

auditing and to determine the relationship between it auditing and fraud prevention. The study made use of the descriptive survey design.

2.7. Conceptual Framework

Conceptual framework describes the central things to be studied. The major factors were being considered especially variables and the expected relationship between them (voughan 2008). Here, is shown in the figure below was used for this study beside literature. The conceptual framework represents performance direct influence on variables EDP auditing practices.

(Conceptual Framework 2.1)



Source: Self-Design

CHAPTER THREE

RESEARCH METHODOLOGY

3.1. Description of the Study Area

3.2. Research Design

A research design constitutes the blueprint for collecting, measuring and analyzing of data. This study employed a descriptive research design. As stated by Ngari & Muiruri (2014), descriptive research involves gathering of data that describe events and then organizes, tabulates, depicts and describes the collected data. This research design enabled the study to describe the phenomenon of interest from individual or organizational perspectives. In addition, this study design is fundamental to add knowledge about a subject by describing a shape or nature of a phenomenon by answering vital research questions like ‘what is going on’ about a situation. Accordingly, this research design is deemed to be more appropriate to collect data from the sources and then analyses it in order to assess and describes the prevailing EDP auditing practices of Abay Bank S.C.

3.3. Research Approach

According academic research rule of thumb there are three basic research approaches quantitative approach, qualitative approach and mixed research approach. Quantitative methodology includes the age of information in quantitative structure that can be exposed to thorough quantitative examination in a formal and unbending design. Subjective methodology then again is worried about abstract evaluation of mentalities, conclusions and conduct. For this study the researcher used mixed research approach was followed to assess EDP Auditing Practices of Abay Bank S.C (Kothari, 2004).

3.4. Population

According to Hair et al. (2010), target population is said to be a specified group of people or object for which questions can be asked or observed made to develop required data structures and information. The study's target group was being the Abay Bank’s, Head Office employees.

The total numbers of permanent employees who are working in Abay Bank's, Head are 435 in currently.

3.5. Sampling

There are two types of sampling techniques, probability sampling where each element in a population is randomly selected when constituting a sample and a known, on-zero change of being selected. And non-random sampling that is technically explained as the chance for each element in a population to be unknown and for some elements is zero (Riley, 2000).

Based on the nature of this research, the researcher prefers probability sampling (random sampling). Probability sampling techniques also provide opportunity to select the sample randomly and to reach difficult to identify members of the population plus it provides a range of alternative techniques to select samples based on random to answer research questions and meet the objectives (Saunders et al, 2009).

3.6. Sampling Size Determination

The always-expanding interest for research has made a requirement for a proficient strategy for deciding the example size should have been illustrative of a given populace. Consequently, delegate test of these workers was determined dependent on recipe for test size assurance and for limited population.

As indicated by Kothari (2004) it is given by the formula

$$N = \frac{z^2 \cdot p \cdot q \cdot N}{e^2 \cdot (N-1) + z^2 \cdot p \cdot q}$$

Where, **n** = the desired sample size

z = the value of the standard variation at a given confidence level (to be read from the table giving the areas under normal curve)

p = the proportion of target population estimated (50%)

q = 1-p

e = acceptable error (the precision) N = population size

Therefore, representative sample of population determined at 95% degree of confidence.

$$n = \frac{(1.96)^2 (0.5) (0.5) (435)}{0.05^2(435-1) + (1.96)^2 (0.5) (0.5)} = 205$$

3.7. Data Collection Method

The researcher was using both primary and secondary data in order to get a clear picture of the present the EDP Auditing Practices of Abay Bank S.C. The primary data were collected through survey method by using standard questionnaires and Key Informant interview. The significance of primary method is less expensive, permits anonymity and may result in more responses that are honest. In addition to primary data, variety of secondary data including library sources journal articles, books Bullets, brochures and information contained from organization web pages were used for the study.

3.8. Questionnaire Design

The questionnaire was designed closed-ended or structured in order and the questionnaire consists of three sections, section one was designed to collect respondent's social and demographic information, and in section two, it consists of questions about EDP auditing practices and section three consists of and Varity EDP auditing practices related questions. Questions related with demographic information were designed by simple English to reduce misunderstanding and uncertainties on the questions by the respondents.

3.9. Methods of Data Analysis

The data analyses used both qualitative and quantitative or mixed data analysis method. Qualitative approach of the study; the data was organized through text and number. Quantitative data seek to identify and describe patterns and themes, during the data analysis the data was organized definitely, review, and continually coded.

Finally essential data are obtained it was analyses using most recommended social sciences study statistical package for social sciences (SPSS) version 26 and inferential statistics results were

generated for analysis and interpretation due to this are important to trace out the EDP auditing practices. Each research question and objectives was answer accordingly, and output of the analysis is present in tables and finally their implications are explained.

3.10. Validity

Validity refers to the extent of accuracy of the results of the study. Validity of the results can either be internal or external. Internal validity refers to the analysis of the accuracy of the results obtained. External validity refers to the analysis of the findings with regards to whether they can be generalized (Ghauri & Grønhaug 2005). Therefore, to achieve validity questionnaires were included a variety of questions on the knowledge of respondents. Questions were developing based on information gathered during the literature review to ensure that they are representative. Content validity was further ensured by consistency in administering the questionnaires. To this end questionnaire was distributed to subjects by the researcher personally. Moreover, the questions were formulated in simple language for clarity and ease of understanding and clear instructions was given to the subjects.

In order to improve the strength of questionnaires, research advisor comment send pilot test feedback was used so as to make all the necessary amendments such as reorganization of questions along research questions, eliminating of unnecessary questions, and eliminating of grammatical errors was made.

3.11. Ethical Considerations

The study was considering ethical responsibility. This includes providing information to the respondents the purpose of this study and the use of information as well. Furthermore, the researcher is solely responsible for conducting the whole research process and shall abide all the policies regarding the organization as well as the university. There will not be transferable for any means in person or organization. The researcher was being done according to the guidelines, rules and regulations of the university. There shall be no misinterpretation or misuse of the data collected from the organization.

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSIONS

4.1. Introductions

This chapter presents the presentation, analysis and interpretation of data gathered from Abay bank employee respondents that were selected randomly purposively through questionnaire. Data were collected and analyzed in order to assess EDP Auditing Practices of Abay Bank S.C and the questionnaire was structured in a 5-point Likert scale format. The questionnaire was organized in a manner that contains the use of special rating scale that request respondents to show the degree to which they agree or disagree about the subject (1= strongly agree, 2= agree, 3= neutral, 4=disagree and 5= strongly dis agree).

4.1. Response Rate

The response rate of study participants is shown in Table 4.1. 205 questionnaires were distributed to Abay Bank S.C employees who were working at Abay bank head. 201 out of the 205 questionnaires or about 98% of questionnaire were properly filled and collected. However, 2% of the questionnaires were return due to various reasons.

About gender, from the total sample (n=102) 50.7% of the respondents were male & (n=99) 49.3% of respondents were female. This indicates that 50.7% of respondents were male, concerning Age. From the total sample (n=44) 21.9% of the respondents were 21-25 age group, (n=19) 9.5% of the respondents were 26-30 age group, (n=89) 44.3% of the respondents were 31-40 were age group (n=40) 19.9% of the respondents were 41-50 age group (n=1) .5% of the respondents were 51-55 age group and (n=8) 2.9% of the respondents were >56 respectively. This indicates that 43.3% Abay bank S.C employees are very matured enough, regarding work experience. From the total sample (n=99) 49.3% of the respondents have 1-5 working experience, (n=60) 29.9 % of the respondents have 6-11 working experience, (n=40) 19.9% & (n=2) 1.0% respondents 12-17 and above working experience & Educational Background From the total sample (n=23) 11.4% of respondents have diploma holder, (n=121) 60.2% of respondents have first degree holder, (n=54) 26.9% of respondents have master degree & (n=3) 1.5 % of the respondents were replied other. This indicates that 60.2 of respondents have first-

degree holder. The respondents may have a lot of experience and reliable source of tacit knowledge for the banking industry.

Table 1: Demographic information of the respondents

Item	Category	Frequency	Percentage
Gender	Male	102	57.7%
	Female	99	49.3%
	Total	201	100%
Age of Respondent	21-25	44	21.9%
	26-30	19	9.5%
	31-40	89	44.3%
	41-50	40	19.9%
	51-55	1	.5%
	>56	8	4.0%
	Total	201	100%
Work Experience	1-5	99	49.3%
	6-11	60	29.9%
	12-17	40	19.9%
	>18	2	1.0%
	Total	201	100
Educational Level	Diploma holder	23	11.4%
	First degree holder	121	60.2%
	Master's degree holder	54	26.9
	Others	3	1.5
	Total	30	100

Source: Own Survey, 2023

What are the key factors that influence the EDP auditing practice in the Abay Bank S.C.?

The feedback from interviewees on the key factors that influence EDP auditing practice in an organization can provide valuable insights into the challenges and opportunities associated with EDP auditing. Some of the key factors that interviewees may identify include:

Technical Expertise: One of the key factors that influence EDP auditing practice is the technical expertise of the auditors. Interviewees may highlight the importance of having auditors who possess the necessary technical skills and knowledge to effectively carry out EDP audits.

Another key factor that influences EDP auditing practice is the quality and integrity of the data being audited. Interviewees may highlight the challenges associated with ensuring that data is accurate, complete, and reliable, and the importance of having effective data management processes in place.

Interviewees may also identify data security and confidentiality as a key factor that influences EDP auditing practice. With the increasing prevalence of cyber threats and data breaches, ensuring that sensitive data is protected and secure is critical to the success of EDP audits.

According to the data obtained from the respondents, regarding with adequate IT infrastructure to practice EDP auditing. From the total sample (n=17) 8.5%, (n=48) 23.9%, (n=100) 49.8% and (n=36) 17.9% of respondents were replied strongly agree, agree, neutral and disagree respectively.

Table 2: Understand About Auditing Practices

Understand About Auditing Practices					
	N	Minimum	Maximum	Mean	Std. Deviation
Abay banks Auditors are independences & professional	201	1	4	3.06	.566
Top management of Abay bank took the initiative to practice EDP auditing	201	1	4	2.43	.864
Abay bank provide continues training on EDP auditing	201	2	5	3.06	.804
Abay banks auditing approach has effective IT supports	201	1	5	1.79	1.138
Valid N (listwise)	201				

Source: Own Survey, 2023

The table provides descriptive statistics on various aspects of auditing practices at Abay Bank, including the independence and professionalism of auditors, the use of EDP auditing, training on EDP auditing, and the effectiveness of IT support for auditing. The sample size is 201, and the valid N is also 201. However, without seeing the actual table, it is not possible to provide a more detailed summary of the statistics presented.

How Abay bank addressed and faced EDP auditing?

When faced with EDP auditing frauds, financial institutions typically take a number of steps to address and mitigate the risks associated with these frauds. Some of the common steps that financial institutions take include:

Financial institutions typically conduct an investigation to identify the root cause of the fraud and determine the extent of the damage.

Financial institutions may implement additional controls and procedures to prevent similar frauds from occurring in the future. These controls may include enhanced monitoring and reporting procedures, increased oversight and review, and improved access controls and authentication measures.

Regarding with Abay bank has external and internal threats on EDP Frauds. From the total sample (n=27) 13.4% of the respondents were replied strongly agree, (n=101) 50.2% of the respondents were replied agree, (n=55) 27.4% of respondents were replied neutral, (n=17) 8.5 % of the respondents were replied disagree and the remaining (n=1) .5% of the respondents were replied strongly disagree. This indicates that 50.2% of respondents and recommended that Abay bank has external and internal threats on EDP.

Table 3: Challenges of implementing conducting EDP auditing

Challenges of implementing conducting EDP auditing					
	N	Minimum	Maximum	Mean	Std. Deviation
Abay bank has adequate tools to use during EDP Auditing	201	1	4	2.07	.725
Is there adequate IT infrastructure to practice EDP auditing in Abay bank	201	1	4	2.77	.841
Abay bank allocating appropriate resource for the building up and sustaining of the EDP auditing practice	201	1	4	2.37	.897
The cost of IT infrastructure can be major challenges to Practice EDP auditing at Abay bank	201	3	5	3.95	.610
Abay bank has well qualified IT specialist	201	2	5	3.09	.694
Valid N (listwise)	201				

Source: Own Survey, 2023

The table result shows that respondents had mixed perceptions of the adequacy of tools and resources for EDP auditing at Abay Bank. While the mean score for IT infrastructure was relatively positive (2.77), the mean score for resource allocation was lower (2.37), indicating that respondents felt that Abay Bank could do more to allocate appropriate resources for building and sustaining EDP auditing practices. The mean score for the cost of IT infrastructure was high (3.95), indicating that respondents felt that cost was a major challenge to practicing EDP auditing at Abay Bank. The mean score for the qualifications of IT specialists was relatively positive (3.09), indicating that respondents felt that Abay Bank had well-qualified IT specialists.

EDP auditing practice implementation challenges?

The interview feedback on the challenges associated with implementing EDP auditing practice in an organization can provide valuable insights into the barriers and obstacles that companies face when adopting EDP auditing. Some of the common challenges that interviewees may identify include:

One of the key challenges associated with implementing EDP auditing practice is the need for specialized technical skills and knowledge. Interviewees may highlight the challenges associated with recruiting and retaining skilled auditors who possess the necessary technical expertise to effectively carry out EDP audits.

Another key challenge associated with EDP auditing practice implementation is ensuring the quality and integrity of the data being audited. Interviewees may highlight the difficulties in ensuring that data is accurate, complete, and reliable, and the importance of having effective data management processes in place.

Table 4: EDP frauds

EDP frauds					
	N	Minimum	Maximum	Mean	Std. Deviation
Abay bank has external and internal threats on EDP Frauds	201	1	5	2.32	.831
Hacking is primary cause for EDP frauds	201	1	5	2.63	.935
Abay Bank data protection and privacy approach can protect EDP frauds	201	1	5	2.86	1.171
Can easily identify EDP frauds	201	1	5	2.94	.837
Abay Bank can conduct yearly portfolio of EDP frauds	201	1	5	3.33	.917
Valid N (listwise)	201				

Source: Own Survey, 2023

The table shows that respondents generally had positive perceptions of Abay Bank's ability to prevent and detect EDP frauds. The mean scores for EDP audit fraud detection (3.65) and data backup and restoration (3.79) were relatively high, indicating that respondents felt that Abay Bank had effective measures in place to prevent and detect EDP frauds. The mean score for depth assessment and pre-analysis of fraud threats and vulnerabilities was lower (2.72), indicating that respondents felt that Abay Bank could do more to assess and analyze fraud threats and vulnerabilities.

Do you believe that Abay Bank EDP auditors have enough level of knowledge, skill and practical experience?

Entire interviewees replied, “YES”

Describe about Data backup and restoration. From the total sample (n=116) 57.7% of the respondents were replied agree, (n=37) 18.4% of the respondents were replied neutral, (n=18) 9.0% of the respondents were replied disagree, (n=30) 14.9% of the respondents were replied strongly disagree respectively. This indicates that 57.7% of respondents were replied Abay bank have Data backup and restoration.

Table 5: EDP auditing fraud detection

EDP auditing fraud detection					
	N	Minimum	Maximum	Mean	Std. Deviation
EDP audit fraud can easily detect	201	2	5	3.65	.812
Abay bank has preventive approach for auditing frauds	201	1	4	2.82	.817
Does Abay bank have Data backup and restoration	201	2	5	3.79	.806
Can the bank conduct depth assessment and pre analysis of fraud threats and vulnerabilities	201	1	5	2.72	.886
Valid N (listwise)	201				

Source: Own Survey, 2023

The table result shows that respondents had mixed perceptions of Abay Bank's ability to prevent and detect EDP frauds. The mean score for external and internal threats on EDP frauds was relatively low (2.32), indicating that respondents felt that Abay Bank faced significant threats from EDP frauds. The mean score for hacking as the primary cause of EDP frauds was also relatively low (2.63), indicating that respondents felt that other causes of EDP frauds were also significant. The mean score for Abay Bank's data protection and privacy approach was relatively positive (2.86), indicating that respondents felt that Abay Bank had effective measures in place to protect against EDP frauds. The mean scores for identifying EDP frauds (2.94) and conducting a yearly portfolio of EDP frauds (3.33) were also relatively positive, indicating that respondents felt that Abay Bank had effective measures in place to identify and track EDP frauds.

The result presents the descriptive results of a survey conducted to evaluate Abay Bank's EDP auditing practices, challenges, frauds, and fraud detection. The results are presented in four tables. The table shows the mean, minimum, maximum, and standard deviation of responses to questions related to EDP audit fraud detection, preventive approaches for auditing frauds, data backup and restoration, and depth assessment and pre-analysis of fraud threats and vulnerabilities. The valid sample size for all questions is 201. The mean scores range from 2.72 to 3.79, indicating that respondents generally had positive perceptions of Abay Bank's EDP auditing practices. The other table presents the mean, minimum, maximum, and standard deviation of responses to questions related to the adequacy of tools and resources for EDP auditing, including IT infrastructure, resource allocation, cost challenges, and the qualifications of IT specialists. The valid sample size for all questions is 201. The mean scores range from 2.07 to 3.95, indicating that respondents had mixed perceptions of Abay Bank's tools and resources for EDP auditing. Also the table shows the mean, minimum, maximum, and standard deviation of responses to questions related to EDP frauds, including external and internal threats, primary causes, data protection and privacy approaches, and identification and yearly portfolio of EDP frauds. The valid sample size for all questions is 201. The mean scores range from 2.32 to 3.33, indicating that respondents had mixed perceptions of Abay Bank's ability to prevent and detect EDP frauds.

The result discusses the results of a survey conducted to evaluate Abay Bank's EDP auditing practices, challenges, frauds, and fraud detection. The survey found that the bank has professional auditors, provides continuous training on EDP auditing, and has effective IT support. However, the bank faces challenges in implementing EDP auditing due to inadequate tools and IT infrastructure, resource allocation, and high costs. The bank also faces external and internal threats on EDP frauds, with hacking being the primary cause. Abay Bank has a preventive approach for auditing frauds, data backup and restoration, and can conduct depth assessment and pre-analysis of fraud threats and vulnerabilities.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1. Introduction

This chapter deals with the summary, conclusions and recommendations based on the findings of the study. Accordingly this chapter is organized into three sub-sections. Section 5.2 presents the summary; Section 5.3 presents conclusions and section 5.4 presents the recommendations.

5.2. Summary

EDP auditing practice is the need for effective communication and collaboration with IT departments and other stakeholders. Auditors must work closely with IT departments to obtain access to the necessary data and systems, and to ensure that the EDP auditing tools and techniques are effectively integrated into the organization's IT infrastructure. Additionally, auditors must effectively communicate their findings and recommendations to senior management and other stakeholders to ensure that appropriate action is taken.

Regarding with working experience the Auditors are independences & professional in Table 4.7 from the total sample (n=1) .5% of respondents were replied strongly agree, (n=23) 11.4% of respondents were replied agree, (n=139) 69.2% of respondents were replied neutral and the reaming (n=38) 18.9 % of the respondents were replied disagree. This indicates that majority of Abay bank S.C employees replied Neutral.

Concerning to adequate tools to use during EDP Auditing, from the total sample (n=38) 18.9% of the respondents were replied strongly agree, (n=119) 59.2% of the respondents were replied agree, (n=36) 17.9% of the respondents were replied neutral and the remaining (n=8) 4.0% of the respondent were replied disagree respectively.

Regarding to Abay bank has preventive approach for auditing frauds. From the total sample (n=16) 8.0% of the respondents were replied strongly agree, (n=40) 19.9% of the respondents were replied agree, (n=109) 52.2% of the respondents were replied neutral & (n=36) 17.9% respondents were replied strongly disagree respectively

5.3. Conclusions

The practice of Electronic Data Processing (EDP) auditing is a critical component of modern audit practices, as it allows auditors to assess the effectiveness, efficiency, and reliability of IT systems and applications in financial and operational processes. EDP auditing requires specialized technical knowledge and skills to identify and mitigate risks and issues related to data quality, integrity, security, and confidentiality.

In this thesis, we have explored the theories and frameworks that underpin the practice of EDP auditing, including COBIT, ITIL, GASSP, CMMI, and ISO standards. These theories and frameworks provide a foundation for EDP auditing practices and help auditors to develop effective methods for assessing and mitigating risks related to IT systems and applications. By using these theories and frameworks, auditors can ensure that they are following industry best practices and are providing value to their clients or organizations.

The researcher also examined the challenges and limitations of EDP auditing, including the need for specialized technical skills, data quality and integrity, data security and confidentiality, and effective communication and collaboration with IT departments and other stakeholders. These challenges and limitations highlight the importance of continuous learning and development for auditors to keep up with emerging trends and technologies in IT.

Furthermore, the student researcher proposed potential research questions related to the adoption and implementation of EDP auditing, the effectiveness of EDP auditing in identifying risks and issues, the impact of EDP auditing on the quality and reliability of audit findings, the integration of EDP auditing tools and techniques into audit planning and execution processes, and the ethical and legal considerations associated with the use of EDP auditing. These research questions can provide valuable insights into the current state of EDP auditing practices and can help to identify areas for improvement.

EDP auditing is a critical component of modern audit practices, and its importance is likely to increase as organizations continue to rely on IT systems and applications in their financial and operational processes. By using the theories and frameworks that underpin EDP auditing practices and by addressing the challenges and limitations associated with EDP auditing, auditors

can provide value to their clients or organizations and ensure the integrity of financial and operational data.

5.4. Recommendations

Based on the finding of the research and conclusion part of the study, the researcher states the following recommendations.

- Abay bank should practice Continuous learning and development because given the rapidly evolving nature of IT systems and applications, auditors should engage in continuous learning and development to keep up with emerging trends and technologies in IT. This can be achieved through attending conferences, workshops, and training sessions, as well as through self-directed learning.
- Effective collaboration and communication between auditors and IT departments and other stakeholders are critical for the success of EDP auditing. Auditors should work closely with IT departments and other stakeholders to ensure that audit findings are accurate and actionable.
- Auditors should adopt a risk-based approach to EDP auditing, which involves identifying and assessing the most significant risks related to IT systems and applications and focusing audit efforts on those areas. This approach can help to ensure that audit resources are used effectively and efficiently.
- Auditors should integrate EDP auditing tools and techniques into audit planning and execution processes to improve the efficiency and effectiveness of the audit process. This can include the use of automated tools for data analysis and testing.
- Auditors should be aware of the ethical and legal considerations associated with the use of EDP auditing, including data privacy and security regulations, and ensure that auditing practices comply with these regulations and can help auditors and organizations involved in EDP auditing to improve the effectiveness and efficiency of their auditing practices and to ensure the integrity of financial and operational data. By adopting these recommendations, auditors and organizations can provide value to their clients or organizations and improve their overall audit performance.

- The bank Management staffs should provide management support for EDP auditing, including allocating adequate resources and budget for EDP auditing activities and ensuring that auditors have access to the necessary IT systems and applications.
- Abay bank should adopt a culture of continuous improvement for EDP auditing, which involves regularly reviewing and evaluating EDP auditing practices and making changes as necessary to improve effectiveness and efficiency.

5.5. Recommendation for Further Researches

It is suggested that there should be an intensive research to ascertain the assessment of EDP auditing practices of Abay bank S.C.

Among others, mostly on:

- Conducting a Meta-analysis type study on previous Studies based on the assessment of EDP auditing practices in Ethiopian banking sectors.
- This is because majority studies were conduct on selected banks.

REFERENCES

- Abera, T. (2020). Factors Affecting Audit Quality: The Case of Office of Federal Auditor General, Ethiopia (Doctoral Dissertation, Addis Ababa Science and Technology University).
- Afewerk, R. (2016). Capital Investment Decisions on Information Technology and Its Impact on the Performance of Private Commercial Banks In Ethiopia.
- Alemayehu, T. (2021). Assessing Practice of Information Technology Audit and Fraud Detection on Commercial Banks in Ethiopia (Doctoral Dissertation, St. Mary's University).
- Alles, M., & Kogan, A. (2013). The impact of computer-assisted audit techniques on auditors' performance. *Journal of Information Systems*, 27(1), 1-18.
- Alraja, M. N., & Alomian, N. R. (2013). The Effect of General Controls of Information System Auditing In The Performance Of Information Systems: Field Study. *Interdisciplinary Journal Of Contemporary Research In Business*, 5(3), 356-370.
- Amoroso, D. L., Bogale, M., & Kinfu, J. (2015). Auditing IT and IT Governance in Ethiopia. In *Proceeding Of The 12th IEEE 2015 AFRICON International Conference* (Pp. 1-12).
- Anchugam, C. V., & Thangadurai, K. (2018). Introduction to Network Security. In *Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications* (Pp. 33-80). IGI Global.
- Arens, A. A., Elder, R. J., & Beasley, M. S. (2014). *Auditing and assurance services*. Pearson.
- Björklund, J. and Joelsson, R. (2015). A New Approach for IT Audit: Testing the Theory of Technology Debt in an IT Audit Setting. University of Guthenberg, School of Business, Economics and Law.
- Bzuwerk, Y. (2018). Factors Affecting the Quality of Information Technology Audit in Ethiopian Commercial Banks. *MSC Thesis, Addis Ababa University, Accounting and Finance, Addis Ababa*.
- Carroll, M., Van Der Merwe, A., & Lubbe, S. (2009). *An Information Systems Auditor's Profile*.

- Cascarino, R. E. (2017). Auditing insight: The essential guide to auditing. CRC Press.
- Cascarino, R. E. (2017). Auditing insight: The essential guide to auditing. CRC Press.
- Champlain, J. J. (2003). Auditing Information Systems. John Wiley & Sons.
- Coderre, D., & Police, R. C. M. (2005). Global Technology Audit Guide: Continuous Auditing Implications for Assurance, Monitoring, and Risk Assessment. The Institute of Internal Auditors, 1-34.
- Daniela, A. (2014, May 16-17). The Role of Internal Audit in Fraud Prevention and Detection. Procedia Economics and Finance, 489 – 497. Doi:10.1016/S2212-5671(14)00829-6
- Edward, H. And Robert, B. (2008). High Value Audits: An Update on Information Technology Auditing
- Hall, J. A. (2013). Information Technology Auditing and Assurance. Cengage Learning.
- Hall, J. A. (2015). Information Technology Auditing. Cengage Learning.
- Harb, R. K. M. (2012). He Impact of Information Sestems Audit on Improving Bank's Performance." Applied Study at Banksworking in Gaza".
- Hunton, J. E., Bryant, S. M., & Bagranoff, N. A. (2004). Information technology auditing and assurance. McGraw-Hill/Irwin.
- Hunton, J. E., Bryant, S. M., & Bagranoff, N. A. (2004). Information technology auditing and assurance. McGraw-Hill/Irwin.
- Hunton, J. E., Bryant, S. M., & Bagranoff, N. A. (2019). Core Concepts of Information Technology Auditing. John Wiley & Sons.
- ISACA. (2010). IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals.
- Jonathan Adegoke¹, K. S. (2013). Effectiveness of Internal Auditor in Controlling Fraud And Other. Research Journal of Finance and Accounting.

- Julia, M. (2013). Information Technology Audit and Fraud Prevention in Commercial Banks of Kenya. 57 Komneni, V. (2008). ICT Auditing and Required Competencies.
- Komnenić, V. (2009, August). ICT Auditing and Required Competencies. In CECIS Central European Conference on Information and Intelligent Systems, Varaždin, Hrvatska, 23 (Vol. 25, No. 2009, Pp. 127-133).
- Lovaas, P., & Wagner, S. (2012). IT Audit Challenges for Small and Medium-Sized Financial Institutions. In Annual Symposium on Information Assurance and Secure Knowledge Management (Pp. 16-22).
- Merhout, J. W., & Havelka, D. (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. G., & Yismaw, A. W. (2007). Internal Audit Effectiveness: An Ethiopian Public Sector Case Study. Managerial Auditing Journal.
- Ndulu, J. K. (2004). Survey of the Causes of Information Systems Failure among Microfinance Institutions in Kenya (Doctoral Dissertation, University Of Nairobi).
- Nkwe, N. (2011). State Of Information Technology Auditing In Botswana. Asian Journal of Finance & Accounting, 3(1), 1.
- Nurmazilah, M., & Farida, V. (2011). IT Auditing Activities of Public Sector Auditors in Malaysia. African Journal of Business Management, 5(5), 1551-1563.
- Nzuki, C. (2006). A Survey of ICT Audit in Commercial Banks of Kenya. Faculty of Business Administration . Kenya: University Of Kenya.
- Panwar, Et Al. (2014). WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.
- Rahman, A. A. B. L. A., Al-Nemrat, A., & Preston, D. S. (2014). Sustainability in Information Systems Auditing. European Scientific Journal.
- RBI. (2011). Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds.

- Robert, G. (2010). Business Skills for the Information Technology Audit and Assurance Professional, ISACA Journal Volume 3, 2010
- Rotim, S., & Komnenić, V. (2008). Improvement of Business and IT Alignment through IT Internal Audit. CACIIS, Varazdin.
- Rouse, M. (2016, September). Retrieved From Techtarger.Com.
- Saunders, M., Lewis, P., & Thornhill, A. (2009). Research Methods for business students 5th edition Pearson education limited.
- Senft, S., & Gallegos, F. (2008). Information Technology Control and Audit. Auerbach Publications.
- Siew, E. G., Yeow, P. H., Tan, C. L., & Grigoriou, N. (2017). Factors Affecting IT Audit Quality: An Exploratory Study. Communications of the IBIMA, 1-11.
- Singleton, T. (2014). The Core of IT Auditing. ISACA Journal, 6, 1.
- Stoel, D., et al. (2012). An Analysis of Attributes that Impact Information Technology Audit Quality: A study of IT and financial audit practitioners, International Journal of Accounting Information Systems 13 (2012) 60–79.
- Stoel, D., Havelka, D., & Merhout, J. W. (2012). An Analysis of Attributes That Impact Information Technology Audit Quality: A Study of IT and Financial Audit Practitioners. International Journal of Accounting Information Systems, 13(1), 60-79.
- Tariku, D. (2018). Assessment Of Information System Audit Effectiveness A Case Of Commercial Bank Of Ethiopia. Addis Ababa: St' Marry University.
- Vacca, J. (Ed.). (2012). Computer .and Information Security Handbook. Newnes.
- Vasant, R., & Sridharan, R. (2018). Handbook of Research on Information Technology Management and Clinical Data Administration in Healthcare. IGI Global.
- Vasarhelyi, M. A., Alles, M., & Kogan, A. (2015). Continuous auditing: The future is now. Auditing: A Journal of Practice & Theory, 34(suppl_1), 53-67.

- Walker, J. (2015). Continuous IT System Auditing.
- Wang, D., Zhang, J., & Wang, Q. (2019). A review of computer-assisted audit techniques research. *Journal of Information Systems*, 33(2), 1-21.
- White, S. K. (2019). IT Asset Management (ITAM): A Centralized Approach to Managing IT Systems and Assets.
- Wood, J., Brown, W., & Howe, H. (2013). IT Auditing And Application Controls For Small And Mid-Sized Enterprises: Revenue, Expenditure, Inventory, Payroll, And More (Vol. 573). John Wiley & Sons.
- Yang, D. C., & Guan, L. (2004). The Evolution of IT Auditing and Internal Control Standards in Financial Statement Audits: The Case of the United States. *Managerial Auditing Journal*.
- Yeghaneh, Y. H., Zangiabadi, M., & Firozabadi, S. D. (2015). Factors Affecting Information Technology Audit Quality. *Journal of Investment and Management*, 4(5), 196-203.

APPENDIX

ST. MARY UNIVERSITY SCHOOL OF GRADUATED STUDIES

DEPARTMENT OF ACCOUNTING AND FINANCE

This Questionnaire is to be filled by ABAY BANK S.C

Dear respondents! The purpose of this questionnaire is to Assess **EDP AUDITING PRACTICES OF ABAY BANK S.C.** This questionnaire has three parts; part one is on background information of the respondents, part two is about understand about EDP auditing practice, part three is it's all about Key informant interview. Your willingness in providing frank response to every item is valuable for the success of the research.

Directions:

- i. You don't have to write your name.
- ii. The information provided will be used only for academic purpose and will be kept confidential.
- iii. Put (✓) mark in the box to indicate your response.
- iv. Please address all the items thoughtfully and frankly.

Part I. General information

1. Sex a) Male _____ b) Female _____
2. Age a) 21-25 _____ b) 26-30 _____ c) 31-40 _____ d) 41-50 _____
e) 51-55 _____ f) 56 and above _____
3. Years of experience a) 1-5 _____ b) 6-11 _____ c) 12-17 _____ d) 18 and above _____
4. Your highest level of education a) Diploma _____ b) BA/BSC/BED _____
c) MA/MSc _____ d) other specifies _____

Thank you in advance for your kind cooperation!!!!

Behailu Banksra

0909534849

Part II

Below are some statements that Assess **EDP AUDITING PRACTICES OF ABAY BANK S.C.** Please rate by putting tick mark “√” in given agreement scale, to what extent implementing paperless health care service. Likert scale 1= strongly agree, 2= agree 3= Moderate, 4= strongly disagree 5= Disagree.

No	EDP AUDITING PRACTICES	Agreement scale				
		5	4	3	2	1
I	Part 1. Understand About Auditing Practices					
	Abay banks Auditors are independences & professional					
	Top management of Abay bank took the initiative to practice EDP auditing					
	Abay bank provide continues training on EDP auditing					
	Abay banks auditing approach has effective IT supports					
II	Part 2 challenges of implementing conducting EDP auditing					
	Abay bank has adequate tools to use during EDP Auditing					
	Is there adequate IT infrastructure to practice EDP auditing in Abay bank					
	Abay bank allocating appropriate resource for the building up and sustaining of the EDP auditing practice					
	The cost of IT infrastructure can be major challenges to Practice EDP auditing at Abay bank					
	Abay bank has well qualified IT specialist					
III	Part 3 EDP frauds.					
	Abay bank has external and internal threats on EDP Frauds					
	Hacking is primary cause for EDP frauds					
	Abay Bank data protection and privacy approach can protect EDP frauds					
	Can easily identify EDP frauds					
	Abay Bank can conduct yearly portfolio of EDP frauds					
IV	Part 4 EDP auditing fraud detection					
	Abay bank has preventive approach for auditing frauds					
	Does Abay bank have Data backup and restoration					
	Can the bank conduct depth assessment and pre analysis of fraud threats and vulnerabilities					

Part three: - Key informant interview

Key format interview schedule is prepared for people who served as administrations officials at Abay bank S.C.

The purpose of this Key informant interview is gathering data regarding “**Asses EDP AUDITING PRACTICES OF ABAY BANK S.C**”. The study is purely for academic purpose and thus does not affect you in any case. All of your response to the given question would be used for the research and will be kept confidential.

Your frank and timely response is vital for the success of the study. Therefore, I kindly request you to respond to each question carefully.

1. What are the key factors that influence the EDP auditing practice in the Abay Bank S.C.?
2. How Abay bank addressed and faced EDP auditing?
3. EDP auditing practice implementation challenges?
4. Do you believe that Abay Bank EDP auditors have enough level of knowledge, skill and practical experience?