



ST MARY'S UNIVERSITY

SCHOOL OF GRADUATE STUDIES

DEPARTMENT OF ACCOUNTING AND FINANCE

ASSESSMENT OF INTERNAL CONTROL EFFECTIVENESS IN E-BANKING;  
THE CASE OF COMMERCIAL BANK OF ETHIOPIA

BY: - MESERET BEZABIH

ADVISOR: - MISRAKU MOLLA (PH. D)

JUNE 14, 2024

ADDIS ABABA, ETHIOPIA

---


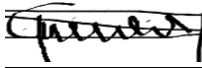
ST. MARY’S UNIVERSITY  
SCHOOL OF GRADUATE STUDIES

ASSESSMENT OF INTERNAL CONTROL EFFECTIVENESS IN E-BANKING: THE CASE  
OF COMMERCIAL BANK OF ETHIOPIA

BY

MESERET BEZABIH

APPROVED BY BOARD OF EXAMINERS

	Name	Signature	Date
Dean, Graduate Studies	_____	_____	_____
Advisor’s Name	<u>Misraku Mola (PhD)</u>	_____	_____
Internal Examiner	<u>Simon Tarekegn (Asst. prof.)</u>		_____
External Examiner	<u>Gidey G/Hiwot (PhD)</u>		<u>July 13, 2024</u>

## Acknowledgment

I would like to extend my deepest appreciation to the entire team at the Commercial Bank of Ethiopia for their unwavering support and collaboration throughout the duration of this research. Their willingness to share insights into the intricacies of E-banking operations and internal control mechanisms has been indispensable to the success of this study.

Special thanks to the CBE internal control department especially Ato Henok within the bank for his generosity in providing time for interviews and offering valuable perspectives that significantly contributed to the depth and accuracy of our analysis.

I am immensely grateful to the participants who willingly participated in interviews, surveys, and other data-collection activities. Their input has been instrumental in capturing the nuanced aspects of E-banking within the context of the Commercial Bank of Ethiopia.

I extend my gratitude to Dr. Misraku Molla my dedicated advisors, for their guidance, mentorship, and constructive feedback throughout the research process. Their expertise has been crucial in shaping the direction and focus of this study.

A sincere thank you to my colleagues and peers for their collaborative spirit, insightful discussions, and the exchange of ideas that have enriched the overall quality of this research.

Furthermore, I would like to express my deepest appreciation to my husband and children for their unwavering support and understanding during the demanding phases of this research project and also my best friends support me in effective paper making. Their encouragement has been my pillar of strength.

In conclusion, this research would not have been possible without the collective efforts, contributions, and encouragement of all those mentioned above. Thank you for being an integral part of this journey towards understanding and enhancing the internal control effectiveness in E-banking at the Commercial Bank of Ethiopia.

Contents	
Acknowledgment .....	ii
Contents .....	iii
LIST OF TABLES .....	vi
List of Figure.....	vii
Acronyms.....	vii
<i>Abstract</i> .....	viii
CHAPTER ONE .....	1
1 Introduction .....	1
1.1 Background of the study .....	1
1.2 The statement of the problem.....	2
1.3 objectives of the study.....	5
1.3.1 General Objectives .....	5
1.3.2 Specific objectives .....	5
1.4 Significance of the study.....	5
1.5 Scope of the study .....	6
1.6 Limitations of the study .....	6
1.7 Organization of the Study .....	7
CHAPTER TWO .....	8
2 Related literature review.....	8
<b>2.1 The Concept of Internal Control</b> .....	8
2.1.1. Importance of Internal Controls.....	9
2.1.2. What is the COSO Framework?.....	10
2.1.3. Components of Internal Control System.....	10
2.1.4. How is the COSO Framework used? .....	14
2.1.5. What are the benefits and limitations of the COSO Framework?.....	14
2.1.6. Types of internal controls.....	15
2.1.7. Internal controls in the banking sector .....	18
2.1.8. Electronic Banking Overview .....	19
<b>2.2 Empirical Literature Review</b> .....	19

2.2. Research Gap .....	20
CHAPTER THREE.....	21
3. Research Methodology .....	21
3.1. Introduction.....	21
3.2. Research Design.....	21
3.3. Population and Sampling .....	21
3.4. Data collection method .....	22
3.5. Method of data analysis .....	22
3.6. Ethical considerations .....	23
CHAPTER FOUR.....	24
4. Data analysis and discussion.....	24
4.1. INTRODUCTION .....	24
4.1.2. Gender Distribution of Respondents.....	25
4.1.3. Age of the respondents.....	26
4.1.4. Year of service in the bank.....	27
4.2. Control environment of internal control systems.....	29
4.2.1. Integrity and ethical values related to E-banking.....	29
4.2.2. The development and performance of internal control related to E-banking.....	30
4.2.3. Reporting lines, and appropriate authorities and responsibilities .....	32
4.2.4. to attract, develop, and retain competent .....	32
4.2.5. internal control responsibilities related to E-banking .....	34
4.3. Risk assessment of internal control systems .....	36
4.3.1. the identification and assessment of risks relating to E-banking .....	36
4.3.2. Objective achievement across the entity and analyzes risks .....	36
4.3.3. The potential for fraud in assessing risks related to the achievement of E-banking objectives. ....	38
4.3.4. The significant impact of the internal control for E-banking.....	40
4.4. Control activities of internal control systems.....	41
4.4.1. To the mitigation of risks related to E-banking to acceptable levels.....	42
4.4.2. General control activities over technology to support the achievement of E-banking objectives .....	43
4.4.3. Deploys control activities through policies.....	45

4.5.	Information and communication.....	47
4.5.1.	Relevant, quality information to support the functioning of internal control over E-banking. 48	
4.5.2.	To support the functioning of internal control specific to E-banking. ....	49
4.5.3.	External parties regarding matters affecting the functioning of internal control over E-banking 51	
4.6.	Monitoring Activities .....	54
4.6.1.	the components of internal control related to E-banking are present and functioning.....	54
4.6.2.	For taking corrective action .....	56
CHAPTER FIVE .....		58
5.1.	Introduction.....	58
5.2.	Summary of the Study .....	58
5.3.	Conclusion .....	60
5.4.	Recommendation of the study.....	61
References.....		65
References		
Annexes		

## LIST OF TABLES

Table 4.1.1. employee's current position .....	24
Table 4.1.2. Sex Distribution of Respondents.....	26
Table 4.1.3. Age of respondents.....	27
Table 4.1.4. Year of Service in the Bank.....	28
Table 4.2.1 integrity and ethical values related to E-banking.....	29
Table 4.2.2 development and performance of internal control related to E-banking.....	31
Table 4.2.3. Clear Structure of Reporting System .....	32
Table 4.2.4. To attract develop and retain E-banking .....	33
Table 4.2.5 Individuals accountability and responsibility .....	34
Table 4.3.1. Strategy for Identifying Risks Effectiveness.....	36
Table 4.3.2. Appropriate Response to Risks .....	37
Table 4.3.3. consider the potential for fraud in assessing .....	38
Table 4.3.4. impact the internal control for E-banking .....	40
Table 4.4.1. to mitigate risks related to E-banking to acceptable levels .....	42
Table 4.4.2. selects and develops general control activities .....	44
Table 4.4.3. deploys control activities through policies established by the bank procedures.....	45
Table 4.5.1. relevant, quality information to support the functioning .....	48
Table 4.5.2. support the functioning of internal control specific to E-banking. ....	49
Table 4.5.3. External parties regarding matters affecting the functioning .....	52
Table 4.6.1. The component of internal control related to E-banking .....	54
Table 4.6.2. taking corrective action .....	56

List of Figure	
Figure 1: Conceptual framework .....	26.
(COSO internal control framework)	

## Acronyms

NBE - NATIONAL BANK OF ETHIOPIA

CBE- COMMERCIAL BANK OF ETHIOPIA

COSO- COMMITTEE OF SPONSORING ORGANIZATION

AICPA - AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

E-BANKING- ELECTRONIC BANKING

IC - INTERNAL CONTROL

ICAEW- INSTITUTE OF CHARTERED ACCOUNTANTS OF ENGLAND AND WALES

IAG - INTERNATIONAL AUDITING GUIDELINES

INTOSAI: -INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONs

## *Abstract*

*This study focuses on evaluating the internal control effectiveness of E-banking operations within the Commercial Bank of Ethiopia (CBE). The assessment was made based on the five components of the COSO internal control framework. The study used a descriptive research design. The study makes use of primary data that are collected using closed-ended questionnaires. The study finds the following results. First, concerning control environment of internal control, a significant majority of respondents perceived the existence of a clear separation of roles and responsibilities in the CBE's E-banking operations. Second, the majority of respondents recognized the importance of considering risk assessment for fraud in assessing risks related to E-banking objectives. There was a positive perception that the bank identifies and assesses changes that could significantly impact internal control for E-banking. Third regarding control activities respondents strongly agreed that the bank has selected and developed general control activities over technology to support the achievement of E-banking objectives. The bank deploys control activities through policies and procedures effectively, ensuring transparency and compliance. Four concerning information and communication practices, the study finds that the bank generates and utilizes relevant, quality information to support internal control E-banking. The bank effectively communicates objectives and responsibilities for internal control within the organization and with external parties. Finally, regarding monitoring activities and evaluation, the study find that the bank conducts ongoing evaluations to ascertain the presence and functioning of internal control components and communication deficiencies promptly to relevant parties for correction action.*

*Keywords: COSO internal control framework, control environment, risk assessment, control activities, information and communication, monitoring activities and evaluation, CBE*

# CHAPTER ONE

## 1 Introduction

### 1.1 Background of the study

The financial sector is commonly perceived as a significant part of the economies of all nations, considering the role it plays in promoting growth and development, saving, cash flow regulation, foreign exchange, trade, investment, and so on. Therefore, in planning its growth and development nations pay close attention to the financial sector. (Adewale,2014)

In the dynamic landscape of modern banking, the integration of electronic banking(E-banking) services has become ubiquitous, reshaping the way financial institutions operate and customers engage with their services. This paradigm shift brings to the forefront the critical importance of robust internal controls to ensure the security, integrity, and efficiency of the E-banking system.

Internal control in financial institutions, especially banks refers to the process and procedures put in place to ensure the reliability of financial reporting, compliance with laws, and the effectiveness and efficiency of operations. This includes measures to safeguard assets, prevent fraud and error, and ensure the accuracy and completeness of financial records. Internal control also involves the segregation of duties, regular monitoring and supervision, and the implementation of risk management practices to mitigate potential threats to institutions' financial stability. Assessing these areas of internal control in commercial banks helps to ensure the reliability of financial reporting, compliance with laws and regulations, and overall soundness of the bank's operations. (Adewale,2014).

internal control in E-banking is relevant and important E-banking involves unique risks and challenges. Such as cybersecurity threats and the need for secure online transactions. Assessing internal controls in E-banking can help to ensure the security of customer data, prevent fraud and unauthorized access, and maintain the integrity of financial transactions, additionally, evaluating internal controls in E-banking can help to ensure compliance with regulations related to

electronic financial services. Overall, it's a valuable area of study for understanding how commercial banks manage and mitigate risks in their digital operations. (COSO,2014)

This study is aimed to assess the effectiveness of internal control in E-banking in CBE. The remaining part of this chapter is the statement of the problem, research questions, objectives of the study, scope of the study, the significance of the study limitation of the study and also organizational study.

## 1.2 The statement of the problem

Banks play a vital role in an economy as they hold the savings of the public to provide a means of payment for goods and services and finance the development of business. The globalization of the economy, technological advancements, complexity of business, and allegations of fraudulent financial reporting have recently sharpened the ever-increasing attention on internal controls and internal auditing, (Bowrin,2004).

Effective internal control for all organizations especially in the bank the first crucial need for the financial sector for the stability of the organization is strong internal control, so every financial sector has to have a strong internal control system.

That helps the strength, reliability, trust, and other relevant things. In e-banking services, the bank must have a strong internal control system. because of technological advancement fraud increases day to day by very high so the financial sector maintains a very strong internal control system.

In addition, COSO posits that ICS ensures management fulfills their duties to stakeholders in the right manner; ensures transparency in financial statements, and is law-abiding (COSO, 2014). High-profile company failures usually result in the imposition of further rules and necessities and subsequent long and expensive compliance efforts. Per the New York State Control Task Force Report, the basic principles of IC are frozen in well-structured organizational techniques and principles. Effective IC also fabricates a competitive advantage, as an organization with effective

controls stands the chance of managing any risk effectively. A viable internal control framework is the essential mainstay of all organizations everything being equal, the breakdown of which will cost the organization hugely. Internal control systems should be the key relevant aspect of an organization's policies globally. The revision of the 1992 internal control framework (COSO, 1992) of COSO in 2013 was necessary due to the global change in business models. Organizations without or with weak ICS cannot survive as stated in the 1987 report of the Treadway Commission, the lack of effective IC is the basic cause of fraudulent financial reporting of companies (Asiligwa & Rennox, 2017).

Recently in our country the Commercial Bank of Ethiopia lacks a strong internal control system in E-banking. The Commercial Bank of Ethiopia recently announced commercial bank of Ethiopia lost over 801 million birrs by fraud, all financial service fraud happens through electronic channels, therefore, this paper intends to review the internal control measures essential in preventing electronic banking fraud in the banking sector.

Olatunji (2009) investigated the impact internal control system on the banking sector of Nigeria. The results of the study show that ICS is very important in the prevention and detection of fraud in the banking sector of Nigeria. Amudo et al. (2009) identify the six essential components of an effective internal control system; control environment, risk assessment, control activities, information and communications, monitoring, and information technology in their study. The findings of the study under evaluation results are that measuring effectiveness of internal control is concerned with the existence and functioning of the six major control components identified by the model. Using mixed research approach, Tekalign (2018) assesses the effectiveness of the internal control system in the commercial bank of Ethiopia case of Hawassa City. The study finds that the company's internal control is effective in terms of having clear codes of conduct, management of the company periodically reviews policies and procedures; sets clear objectives, this is communicated to all staff for direction on risk assessment; there is an adequate and strong dual control and separation of duties in the organization and there is effective reporting procedure in the organization and this also communicated to employees.

Effective internal controls contribute to better performance by financial institutions. The success of the system depends on a positive internal control culture. Banks should have in place a comprehensive internal control management process to identify; measure, monitor, and control internal control system effectiveness and compliance. There is also a need for financial institutions to cultivate a culture of ethically doing business from the top management which should see this culture cascading down to the most junior worker or employee in the organization to promote adherence to internal controls of the organization which are essentially management tools on measuring compliance to an organization way of doing business in a competitive environment. (Kosmas Njanike, 2011)

The study done by Douglas, 2011 considered the control environment, risk assessment, information and communication system, and control and monitoring activities as independent variables, and internal control effectiveness as a dependent variable to evaluate the internal control effectiveness in Ecobank Ghana Limited Ashanti Region.

However, these prior studies simply assess and evaluate the overall internal control system of banks. Studies that assess internal control in E-banking is very limited. Internal control in E-banking is relevant and important E-banking involves unique risks and challenges. Such as cybersecurity threats and the need for secure online transactions. Assessing internal controls in E-banking can help to ensure the security of customer data, prevent fraud and unauthorized access, and maintain the integrity of financial transactions, additionally, evaluating internal controls in E-banking can help to ensure compliance with regulations related to electronic financial services. Thus, this study aimed to assess the internal control effectiveness of CBE particularly related to E-banking using COSO internal control framework.

The following research questions need to be addressed

1. Is there a safe and secure online banking system?
2. Does the online banking system catch mistakes or fraud?
3. Are financial reports accurate and trustworthy?

4. Do all users, like customers and bank employees, get important information about online banking safety?

5. How does the online banking system check for problems or mistakes?

6. Are there consistent rules to keep online banking safe and secure?

### 1.3 objectives of the study

#### 1.3.1 General Objectives

The general objectives of the study are to evaluate the effectiveness of internal control in E-banking in the case of the Commercial Bank of Ethiopia using COSO internal frameworks.

#### 1.3.2 Specific objectives

This study had addressed the following specific objective

- To evaluate the risk assessment practice related to e-banking.
- To assess the controlling activities towards e-banking service.
- To examine information and communication practices related to e-banking services.
- To identify the monitoring related to e-banking service.

### 1.4 Significance of the study

The significance of this research lies in its potential to contribute actionable insights that can shape the future of E-banking services at the Commercial Bank of Ethiopia. By identifying areas for improvement in internal control mechanisms, the study aims to empower the bank to proactively address emerging risks, ensuring the resilience and sustainability of its E-banking operations. As the banking sector continues its digital evolution, findings from this study hold relevance not only for the commercial Bank of Ethiopia but also for the broader financial industry. The study strives to fill existing gaps in the understanding of internal control effectiveness in E-banking offering practical recommendations that can drive positive change in the realm of digital financial service. Also, there is no exact paper from this title of assessment of internal control effectiveness of in E-banking the case of the commercial Bank of Ethiopia in the country.

## 1.5 Scope of the study

The scope of this research is delimited to the assessment of internal control effectiveness in e-banking service at the Commercial Bank of Ethiopia.

- Geographical scope: this research had focus exclusively on the operation of the Commercial Bank of Ethiopia, considering its unique position within the Ethiopian banking sector.
- Subject scope: the study had concentrated on internal controls related to electronic banking services, including but not limited to online transactions, mobile banking, and other digital financial platforms offered by the Commercial Bank of Ethiopia.
- Methodological scope: the research had analyzed and evaluate the existing internal control mechanisms, emphasizing their effectiveness in mitigating risks associated with e-banking operations using the COSO internal control framework.

## 1.6 Limitations of the study

While this research aims to provide valuable insights into the assessment of internal control effectiveness in E-banking at the commercial bank of Ethiopia, certain limitations should be acknowledged:

- Data availability: The study relies on the availability and accessibility of accurate and comprehensive data related to internal controls, historical incidents, and customer feedback.
- Access to Internal Processes: Full access to internal processes and procedures of the Commercial Bank of Ethiopia may be restricted due to confidentiality concerns. This limitation could affect the granularity of the assessment.
- External Factors: External factors, such as changes in regulatory frameworks, economic conditions, or technological advancements, could influence the effectiveness of internal controls. These factors may not be fully controllable or predictable.
- Emerging Risks: The identification of emerging risks is inherently challenging, and the study's ability to predict future threats to the internal control framework may be limited.

- Acknowledging these limitations is crucial for interpreting the study's results and conclusions. The research will strive to mitigate these constraints to the best extent possible, ensuring the validity and reliability of the findings within the defined scope.

### 1.7 Organization of the Study

The research paper has five chapters; the first chapter has included background of the study, statement of the problem, research questions, objectives, significance and scope of the study. The second chapter is about literature review which is related to the study area and it gives a detail description of the study phenomenon by relating other scholar papers on the area. The third chapter is all about methodology of the study in which research approach and method, sources of data, sampling techniques and procedure, method of data collection and analysis and the like has been included. In the fourth chapter the collected data analyzed, discussed and interpreted. And the last chapter contained conclusion, recommendation, references and annex (if any).

## CHAPTER TWO

### 2 Related literature review

This chapter provides a detailed discussion of the conceptual and empirical review of internal control effectiveness in electronic banking in the case of financial institutions, especially banks. In detail discuss internal control definitions, the need for internal control, the importance of internal control, the use of internal control, and also different theories of internal control.

In the empirical review parts, different authors describe their strengths and weaknesses.

#### **2.1 The Concept of Internal Control**

Internal Control implies the whole system of control employed by the management to carry on the business of the enterprise in an orderly and efficient way by having an automatic check and balance overall the transactions. It includes internal checks, internal audits, and other devices of control. An internal control system assures the management that the information it receives is both reliable and accurate. The system also helps to ensure that assets are secure and management policy is being followed properly. Its efficient working not only guarantees management as to the reliability of accounting information, independent auditors also rely on the system of internal control in determining the timing, nature, and extent of the audit work. *(Ravinder Kumar, Virender Sharma, 2005).*

It would be tough for any organization to protect its assets, rely on its records, or operate efficiently if a sound internal control system is absent. Whittington and Pany (2001) state that the Committee of Sponsoring Organizations (COSO) defined internal control as a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories: reliability of financial reporting; effectiveness and efficiency of operations; and compliance with applicable laws and regulations.

The Institute of Chartered Accountants of England and Wales (ICAEW) defined internal control as not only internal checks and internal audit but all systems of control both financially and otherwise, established by the management of an organization to safeguard its assets and promote operational efficiency.

International Auditing Guidelines (IAG) defined internal control as the whole system of control, financial and otherwise established by the management to carry on the business of the enterprise in an orderly and efficient manner, ensure adherence to management policies, safeguard the asset and ensure as far as possible the completeness and accuracy of records.

The internal control system as viewed by the American Institute of Certified Public Accountants (AICPA) is the plan of organization and all the coordinated methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency and encourage adherence to prescribed managerial policies (Obaseki, 2006).

According to Ingram (2009), internal control is the technique employed by managers to ensure that specific control objectives are continuously met. Damagum (2005) puts, it simpler, as any mechanism that the management of an organization puts in place to ensure adequate protection of the organization's assets against illegal use, theft, and other fraudulent abuses. From the above definitions of the concept of internal control, it is clear that internal control systems are medium (not ends on their own but a means to an end) through which organizations ensure smoothness in all their internal dealings as well as with outsiders.

### 2.1.1. Importance of Internal Controls

- evaluate a company's internal controls, including its corporate governance and accounting processes.
- Ensure compliance with laws and regulations as well as accurate and timely financial reporting and data collection. They help to maintain operational efficiency by identifying problems and correcting lapses before they are discovered in an external audit.

- Internal audits play a critical role in a company's operations and corporate governance, now that the Sarbanes-Oxley Act of 2002 has made managers legally responsible for the accuracy of its financial statements.
- No two systems of internal controls are identical, but many core philosophies regarding financial integrity and accounting practices have become standard management practices. While they can be expensive, properly implemented internal controls can help streamline operations and increase operational efficiency, in addition to preventing fraud.

**Importance of Internal Controls** These internal controls can ensure compliance with laws and regulations as well as accurate and timely financial reporting and data collection. They help to maintain operational efficiency by identifying problems and correcting lapses before they are discovered in an external audit.

### 2.1.2. What is the COSO Framework?

The COSO Framework is an industry-standard model for evaluating and implementing internal control systems within organizations. COSO stands for the Committee of Sponsoring Organizations of the Treadway Commission, a private-sector organization that develops frameworks and guidance on organizational governance, internal controls, risk management, and financial reporting.

The framework gives organizations a structure for managing risks and ensuring the reliability of financial reporting. It emphasizes the importance of internal controls; the procedures and processes organizations should use to safeguard assets and improves the accuracy of financial records.

### 2.1.3. Components of Internal Control System

Internal control varies significantly from one organization to the next, depending on such factors as their size, nature of operations, objectives, and the extent of geographical coverage. However,

certain features are essential in considering the components that make up an internal control system.

The Committee of Sponsoring Organizations (COSO) stands on the framework of a good internal control system, including five components: the control environment, risk assessment, the (accounting) information and communication system, control activities, and monitoring. From a general perspective, internal control systems in organizations can be developed around the following basic components; - Internal Audit - Internal Checks (checks and balances); and - Physical Control (Damagum, 2005).

## I. Control environment

The literature suggests that at the heart of effective control is the control environment component. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure, and has a pervasive influence on risk assessment, establishment of objectives, control activities, information and communication systems, and monitoring activities (COSO, 1994). The control environment reflects the board of directors and management's commitment to internal control. It provides discipline and structure to the control system.

## II. Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed and managed. COSO (1994) describes risk assessment as the identification, measurement, and analysis of risks, internal and external, controllable and uncontrollable, at individual business levels and for the bank as a whole.

Management therefore must assess all risks facing the bank because uncontrolled risk-taking can prevent the bank from reaching its objectives or can jeopardize its operations. Effective risk

assessments help determine what the risks are, what controls are needed, and how they should be managed. Management establishes activity-level objectives and mechanisms for identifying and analyzing risks related to their achievement (COSO, 1994).

### III. Control Activities

COSO (1994) described control activities as the policies, procedures, and practices established to help ensure that bank personnel carry out board and management directives at every business level throughout the bank. These activities help ensure that the board and management act to control risks that could prevent a bank from attaining its objectives.

Control activities occur throughout the organization, at all levels, and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties (COSO, 1994).

### IV. Information and Communication

On the other hand, according to COSO (1994) accounting information, and communication systems capture and impart pertinent and timely information in a form that enables the board, management, and employees to carry out their responsibilities. Accounting systems are the methods and records that identify, assemble, analyze, classify, record, and report a bank's transactions. Information and communication systems enable all personnel to understand their roles in the control system, how their roles relate to others, and their accountability. Information systems produce reports on operations, finance, and compliance that enable management and the board to run the bank. Communication systems impart information throughout the bank and to external parties such as regulators, examiners, shareholders, and customers.

Every enterprise must capture pertinent information-financial and non-financial, relating to external and internal events. Relevant information must be delivered to people who need it in a form and timeframe that enables them to carry out their responsibilities and make decisions.

Information is identified, captured, and communicated in a form and timeframe to enable people to carry out their responsibilities (COSO, 1994). Management's ability to make appropriate decisions is affected by the quality of information; that implies that the information should be appropriate, timely, current, accurate, and accessible. Information systems need to produce reports that contain operational, financial, non-financial, and compliance-related information. Effective communication should occur in all directions –flowing down, across and up the organization, throughout all departments and divisions. Management should be kept up-to-date on performance, development, risks, and other relevant events and issues. Management should communicate to its staff what information it needs to be effective, and provide feedback and direction. (COSO 2014)

## V. Monitoring

Monitoring ensures that the internal controls operate as intended over time, and is accomplished through routine (ongoing) activities, separate evaluations, or a combination of both. An effective accounting system will identify and record all valid transactions in the proper time using appropriate classifications and will present those transactions properly in the financial statements.

According to COSO (1994), internal control systems and the application of controls change over time. This can be due to the arrival of new personnel, varying effectiveness of implementing the procedures or supervision, time and resource constraints, or changes in the circumstances for which the internal control system originally was designed. Monitoring is defined as the process that assesses the quality of the system's performance over time which includes ongoing monitoring activities and separate evaluations.

The COSO framework also states that the management of an organization has the ultimate responsibility for ensuring a working internal control system in the organization, with the CEO being the most important individual given the integral part the holder of this position plays in creating a good control environment. However, in the COSO-model the responsibility for the internal control system cannot be limited to the leading positions of the organization – “internal

control is, to some degree, the responsibility of everyone in an organization” (COSO, 1994). Furthermore, the framework identifies external parties such as regulators and external auditors that might contribute to the achievement of the organization’s objectives and provide information that helps internal control. These external parties are however generally not to be held responsible for the internal control in the organization.

#### 2.1.4. How is the COSO Framework used?

The COSO Framework is heavily used by publicly traded companies and accounting and financial firms. The framework seeks to put internal controls in place that formalize the way in which key business processes are performed. This helps organizations to adhere to legal and ethical requirements, while also focusing on risk assessment and management. In addition to integrating such controls into key business processes, the framework places a heavy emphasis on monitoring and reporting, especially as it relates to using internal auditors to monitor adherence to established controls.

#### 2.1.5. What are the benefits and limitations of the COSO Framework?

One of the primary benefits to implementing the COSO Framework is that it helps business processes to be performed in a uniform manner according to a set of internal controls. Depending on how these controls are designed, they can improve efficiency while also reducing risks.

Another benefit is that an organization that fully employs the COSO Framework is often in a better position to detect fraudulent activity, whether that activity is perpetrated by cyber criminals, customers or trusted employees. Because the framework focuses on risk mitigation and adherence to established best practices, vulnerabilities can be significantly reduced.

Finally, some organizations find that when they implement carefully crafted internal controls, it helps them to make existing business processes more efficient. This can help reduce costs and make the organization more profitable.

Despite the benefits associated with implementing the COSO Framework, it is not without its limitations. The most significant of these limitations is that the framework can be difficult to implement for two main reasons. First, the framework is relatively broad in scope, which means that it can be applied to a wide variety of organizations and processes. But this broad scope also means that the framework lacks a significant amount of prescriptive guidance.

The second limitation that can make the framework difficult to apply is its organizational structure. The COSO Framework is broken into a series of rigid categories. Organizations often find that certain processes could conceivably fall into multiple categories, or that do not align well with any of the categories. As such, organizations will often have to make some tough decisions when implementing the framework.

#### 2.1.6. Types of internal controls

The International Organization of Supreme Audit Institutions (INTOSAI): Guidelines for Internal Control Standards (1992) describe the main variables of internal controls below.

- Physical controls

These are both Preventive and Detective controls. Security of physical and intellectual assets, physical safeguards, perpetual records, periodic counts/physical inventories, compare counts to perpetual records, and investigate/correct differences. Liquid assets, assets with alternative uses, dangerous assets, vital documents, critical systems, and confidential information must be safeguarded against unauthorized acquisition, use, or disposition. Typically, access controls are the best way to safeguard these assets. Examples of access controls are as follows: locked doors, keypad systems, card key systems, badge systems, locked filing cabinets, guards, terminal locks, computer password, and menu protection, automatic callback for remote access, smart card, and data encryption.

Departments with capital assets or significant inventories should establish perpetual inventory control over these items by recording purchases and issuances. Periodically, the items should be

physically counted by a person who is independent of the purchase, authorization, and asset custody functions, and the counts should be compared to balances per the perpetual records. Missing items should be investigated, resolved, and analyzed for possible control deficiencies; perpetual records should be adjusted to physical counts if missing items are not located. (COSO, 2014)

- Authorization controls

These are mainly preventive controls. They involve but are not limited to issues regarding to Written policies and procedures, limits to authority, supporting documentation, questioning unusual items, rubber stamps, and numbering blank signed forms.

Authorization is the delegation of authority; it may be general or specific. Giving a department permission to expend funds from an approved budget is an example of general authorization. Specific authorization relates to individual transactions; it requires the signature or electronic approval of a transaction by a person with approval authority. Approval of a transaction means that the approver has reviewed the supporting documentation and is satisfied that the transaction is appropriate, accurate, and complies with applicable laws, regulations, policies, and procedures.

Approvers should review supporting documentation, question unusual items, and make sure that necessary information is present to justify the transaction before they sign it. Signing blank forms should never be allowed. Approval authority may be linked to specific amounts. Transactions that exceed the specified amount would require approval at a higher level. Under no circumstance should an approver tell someone that they could sign the approver's name on behalf of the approver.

Similarly, under no circumstance should an approver with electronic approval authority share his password with another person. To ensure proper segregation of duties, the person initiating a transaction should not be the person who approves the transaction. A department's approval levels should be specified in a departmental policies and procedures manual. (COSO, 2014)

- Internal audit control

This is a type of detective control. Broadly defined, an audit is a comparison of different sets of data to one another, identifying and investigating differences, and taking corrective action, when necessary, to resolve differences. Reconciling/auditing monthly financial reports from the Accounting Department (*e.g.*, Statement of Accounts, Ledger Sheets, etc.) to file copies of supporting documentation of departmental accounting records is an example of internal auditing of the organization's books of accounts. This control activity helps to ensure the accuracy and completeness of transactions that have been charged to a department's accounts.

To ensure proper segregation of duties, the person who approves transactions or handles cash receipts should not be the person who performs the reconciliation. Another example of an audit is comparing vacation and sick leave balances per departmental records to vacation and sick leave balances per the payroll system. A critical element of the auditing process is to identify and resolve differences. It does no good to note differences and do nothing about it. Differences should be identified, investigated, and explained and corrective action must be taken. If expenditure is incorrectly charged to a department's accounts, then the approver should request a correcting journal entry; the reconciler should ascertain that the correcting journal entry was posted. Audit reports should be documented and approved by management. (SOX Guidance, 2007)

- Segregation of Duties

This is a Preventive and Detective control that works with the principle of “At least two sets of eyes” whereby no one person should Initiate a transaction and approve the transaction, record the transaction he/she initiated or approved, reconcile balances, handle assets, and review reports.

Segregation of duties is critical to effective internal control. It reduces the risk of both erroneous and inappropriate actions. In general, the approval function, the accounting/reconciling function, and the asset custody function should be separated among employees. When these functions cannot be separated, due to the small department size, a detailed supervisory review of related activities is required as a compensating control activity. Segregation of duties is a deterrent to

fraud because it requires collusion with another person to perpetrate a fraudulent act. (COSO 2014)

### 2.1.7. Internal controls in the banking sector

The importance and functions of internal controls, particularly in the context of finance departments and banking. Internal control in the banking sector is classified depending on its purpose, operational efficiency, benefits of leadership, significance in banking, responsibilities of board and management, and relation with internal audit.

- Depend on the Purpose of Internal Controls: - Ensure integrity in financial reporting, and regulatory compliance and Prevent fraud and irregularities
- Depend on Operational Efficiency: Improve operational efficiencies, Adherence to budgets and policies, and Identification of capital shortages.
- Depend on Benefits of Leadership: Generation of accurate reports for leadership.
- Depend on Significance in Banking: Foundation of safe and sound banking, Safeguarding of the bank's resources, Production of reliable financial reports and Compliance with laws and regulations.
- Depend on Responsibilities of Board and Management: Board and senior management cannot delegate responsibilities for internal control and Regular verification of internal control integrity by senior management.
- Depend on Relationship with Internal Audit: Internal control involves systems, policies, procedures, and processes implemented by the board, management, and personnel. Internal audit provides an independent review to monitor and evaluate the adequacy and effectiveness of internal controls.

The distinction between internal control and internal audit is highlighted, emphasizing that internal control is a broader concept encompassing the overall systems and processes, while internal audit provides an objective review of these controls.

### 2.1.8. Electronic Banking Overview

The evolution of E-banking has been a global phenomenon, reshaping traditional banking services. E-banking is an arrangement between a bank or a financial institution and its customers that enables encrypted transactions over the Internet. Short for electronic banking, E-banking has various types that cater to customers' different requirements, which can be resolved online. E-banking is also helpful for non-financial transactions such as changing your ATM PIN, getting a mini statement, updating your details, balance inquiry, or printing an account statement. Essentially, it refers to any transaction that doesn't involve any movement of funds to or from your account.

## 2.2 Empirical Literature Review

Tekalign (2018) assesses the effectiveness of the internal control system in the commercial bank of Ethiopia case of Hawassa City. His study employed a mixed research design with a quantitative approach. the study finds that the company's internal control is effective in terms of having clear codes of conduct; management of the company periodically reviews policies and procedures; sets clear objectives, this is communicated to all staff for direction on risk assessment; there is an adequate and strong dual control and separation of duties in the organization and there is effective reporting procedure in the organization and this also communicated to employees.

In Nigeria, a study carried out by Olatunji in 2009 investigated the impact ICS has on the banking sector of Nigeria. The study aimed to find out whether effective and efficient ICS is the best control tool for fraud detection and prevention. The results of the study were that ICS is very important in the prevention and detection of fraud in the banking sector of Nigeria (Olatunji,2009). Olatunji (2009) examined the impact of the internal control system in the banking sector and according to the findings; the lack of an effective internal control system is the major cause of bank fraud in Nigeria. It is then concluded that the management of every bank should create and establish a standard internal control system, strong enough to stand against the

wiles of fraud to promote continuity of operations and to ensure the liquidity, solvency, and going concern concept of the bank.

(Amudo et al. 2009) identify the following six essential components of an effective internal control system; control environment, risk assessment, control activities, information and communications, monitoring, and information technology in their study. The findings of the study under evaluation results are that measuring the effectiveness of internal control is concerned with the existence and functioning of the six major control components identified by the model.

One of, perhaps the most prominent, vital components of a bank's structure in the modern banking system is the internal control system in developed or developing countries. Because effective and efficient performance of the system indicates that, the bank operates as desired. Consequently, investors and other customers in the market will prefer to use the services of that bank since they will have confidence and peace of mind about the bank's financial stability (Yavuz, 2002).

## 2.2. Research Gap

Internal control remains a topic of researcher's interest for the last many decades. As a result, several researches are conducted on the various issues of internal control. However, evaluating internal control from the dimension of E-banking is relatively not well explored. Moreover, the use of COSO internal framework in evaluating internal control, especially in the Ethiopian perspective and in the banking, sector was not applied, so far. Therefore, this study was conducted to assess the internal control practice and experiences of CBE, the giant commercial bank using COSO internal control framework. The increasing risk of business failures, technological advancements/Globalization, fraud and altercations that appeared in the financial sector increased the role for effective internal control systems. Therefore, this paper has given emphasis on the internal control process of CBE in order to assess its practical experience of the internal control systems in E-banking.

## CHAPTER THREE

### 3. Research Methodology

#### 3.1. Introduction

This chapter contains the methodology that will be conduct the research. It describes the research design, the population, the sample, data collection how the data will be analyzed.

#### 3.2. Research Design

To achieve the objectives of the study, the descriptive research design was used to allow the researcher to make an appropriate level of conclusion. To do so the researcher collected primary data by using a structured questionnaire which have questions that focused on the effectiveness of internal control systems in electronic banking used by Commercial Banks of Ethiopia. The target population of the study consists of in head office's digital banking internal control department.

This study used a descriptive survey research design. Lavrakas (2008) describes a descriptive survey research design as a systematic research method for collecting data from a representative sample of individuals using instruments composed of closed-ended and/or open-ended questions, observations, and interviews. It is one of the most widely used non-experimental research designs across disciplines to collect large amounts of survey data from a representative sample of individuals sampled from the targeted population. It employs a qualitative research approach based on it intended to evaluate or assess the internal control practices of CBE related to E-banks services.

#### 3.3. Population and Sampling

The target population of the study comprises all staff of commercial banks of Ethiopia's digital products (E-banking) division at the head office. Thus, the study uses census . There are 70 employees which are by different levels as digital internal control officer, senior digital internal control officer, and manager internal control.

### 3.4. Data collection method

The type of data collected was Primary data obtained using closed-ended questionnaires. The questionnaires were distributed for all staff working in E-banking division at CBE's head office. The variables were measured using a like scale with five response categories (strongly agree, agree, neutral, disagree, and strongly disagree). The questionnaire has six sections; part 1 dealt with demographic information such as sex, marital status, educational background, age distribution, and working experience. Part 2 sought information on the control environment of internal control systems in the organization, assessed risk assessment of internal control systems in the organizations, information on control activities of internal control systems and information and communication of internal control systems respectively, and lastly monitoring activities of internal control systems.

The five components of the COSOS internal control must be effectively designed, implemented, and operated together in an integrated manner, for an internal control system to be effective (COSO integrated framework, 1992). Therefore, the objectives of the five sections of the questionnaire starting from section 2 aimed at evaluating and assessing the five components of internal control systems in the organizations. The bank has different procedures and guidelines for applying the effectiveness of internal control so collect from different procedures and guidelines.

### 3.5. Method of data analysis

All data gathered were systematically analyzed. This requires that data gathered from different respondents was encoded uniformly. The data collected through the questionnaire was analyzed through the statistical package for social science (SPSS) 25 software. The data was analyzed with descriptive statistical analysis to provide frequency and percentage for the interpretation of respondents.

### 3.6. Ethical considerations

The researcher has followed ethically acceptable processes throughout the entire research process. The respondents were informed about the purpose of the study before the information was collected, thus conformed to the principle of voluntary and informed consent. In this regard, the names of the respondent's supportive data were disclosed and information wasn't available to any third parties who weren't directly involved in the study. The researcher further considered that all the sources used in this paper had been properly recognized and acknowledged.

## CHAPTER FOUR

### 4. Data analysis and discussion

#### 4.1. INTRODUCTION

This chapter is intended to provide analysis and discussion of results on the collected data by using frequency tables. The responses from the respondents are described and analyzed in two parts such as; the respondents' background/demographic information, control environment of internal control, risk assessment of internal control, control activities of internal control, information & communication systems of internal control, and monitoring activities of internal control.

##### 4.1.1. The Employee's Current Position

In the bank at internal control in E-banking at the head office level, there are 70 employees which are by different levels as digital internal control officer, senior digital internal control officer, and manager internal control

Table 4.1.1. employee's current position

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Digital internal control	40	57.1	57.1	57.1
	Senior digital internal cont.	11	15.7	15.7	72.8
	Manager internal control	19	27.2	27.2	100.0
	Total	70	100.0	100.0	

the distribution of employees within the internal control department of the bank's e-banking division. This distribution provides insights into the staffing levels across different hierarchical positions within the internal control function, which is crucial for ensuring the effectiveness of internal control in banking operations.

- Digital internal control officer (40 employees, 57.1%): This group constitutes the majority of the internal control department. Their role likely involves day-to-day monitoring and implementation of digital controls within the e-banking system. Their high number suggests a strong emphasis on operational oversight and compliance at the operational level.
- Senior Digital Internal Control Officers (11 employees, 15.7%): Although smaller in number compared to digital control officers, this group holds a significant role. They likely oversee the work of digital control officers, provide guidance on complex issues, and assist in formulating and implementing control strategies. Their presence indicates a layer of supervision and expertise within the internal control function.
- Manager Internal Control (19 employees, 27.2%): This group represents the managerial level within the internal control department. Managers are likely responsible for overall strategy, policy formulation, coordination with other departments, and reporting to higher management or regulatory authorities. Their presence ensures that internal control activities align with organizational objectives and regulatory requirements.

#### 4.1.2. Gender Distribution of Respondents

Out of 70 respondents questioned 34.3% were 24 females and 64.7% were 46 males as indicated in table 4.1.2 The Gender distribution showed that both males and females were represented in the study as shown below.

Table 4.1.2. Gender Distribution of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	24	34.3	34.3	34.3
	Male	46	65.7	65.7	100.0
	Total	70	100.0	100.0	

It seems like you're gathering data for an assessment of internal control effectiveness in e-banking, and this particular set of data pertains to the distribution of respondents by sex in that assessment. Let's interpret it in that context:

The breakdown of respondents by sex provides insights into the demographic composition of the sample participating in the assessment of internal control effectiveness in e-banking.

**Female Respondents (24 individuals, 34.3%):** This group represents a significant portion of the sample, indicating that women are actively participating in the assessment. Their perspectives and experiences will contribute to a more comprehensive understanding of internal control effectiveness in e-banking, ensuring that diverse viewpoints are considered in the evaluation process.

**Male Respondents (46 individuals, 65.7%):** The larger representation of male respondents suggests a majority presence in the sample. Their insights and feedback will also play a crucial role in shaping the assessment outcomes. However, it's essential to ensure that the assessment process considers gender diversity and inclusivity to capture a wide range of perspectives and experiences.

### 4.1.3. Age of the respondents

The age of the respondents in the bank has been assessed and indicated in the following table, Table 4.1.3. The majority of the respondents 12.9% between 18-35 years, 82% of the respondents were 36 to 55 years and the rest 3% of them had 12 to 16 years of experience, and the rest

respondents 3% had higher experience in the bank which was above 22 years. This indicates that the majority of the respondents have few years' experience within the bank.

Table 4.1.3. Age of respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-35	9	12.9	12.9	12.9
	36-55	58	82.9	82.9	95.7
	Greater than or equal to 56	3	4.3	4.3	100.0
	Total	70	100.0	100.0	

- Age Group 18-35 (12.9%): This demographic segment represents a smaller portion of the respondents. It might indicate that younger individuals, potentially newer employees or customers, are less represented in the assessment of internal control effectiveness in E-banking.
- Age Group 36-55 (82.9%): This is the largest segment, suggesting that the bulk of respondents fall within the middle-age bracket. It could imply that individuals in mid-career or those who have been using E-banking for a significant period are actively involved in the assessment process.
- Age Group greater than or equal to 56 (4.3%): This is a smaller but still notable segment. It suggests that there are older individuals, potentially senior employees or long-time customers, involved in assessing the internal control effectiveness in E-banking.

#### 4.1.4. Year of service in the bank

The year of service/experience of the respondents in the bank has been assessed and indicated in the following table, Table 4.1.4. The majority of the respondents 51% have less than 5 years of

experience in the bank, 38% of the respondents have 6 to 11 years in the bank, 8% of them has 12 to 16 years of experience and the rest respondents 3% have higher experience in the bank which is above 22 years. This indicates that the majority of the respondents have few years' experiences within the bank.

Table 4.1.4. Year of Service in the Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-5	17	24.3	24.3	24.3
	6-11	45	64.3	64.3	88.6
	morethan12	8	11.4	11.4	100.0
	Total	70	100.0	100.0	

The table provides an overview of the distribution of respondents' years of experience within the bank, likely in the context of assessing internal control effectiveness. Here's the interpretation:

- 1-5 years of experience (24.3%): This group comprises nearly a quarter of the respondents. It suggests that a significant portion of those involved in the assessment are relatively new to the bank, indicating a fresh perspective or potentially less familiarity with the intricacies of the bank's operations.
- 6-11 years of experience (64.3%): This is the largest segment, representing a substantial majority of respondents. It implies that a significant portion of the assessors have a moderate level of experience within the bank. They likely have gained considerable insight into the bank's operations but might still be open to new approaches or improvements in internal control effectiveness.
- More than 12 years of experience (11.4%): This group constitutes a smaller proportion of respondents, suggesting that there are some individuals with more extensive experience

within the bank involved in the assessment. They likely possess deep institutional knowledge and can provide valuable insights into historical practices and challenges. Overall, the majority of respondents have relatively moderate to low years of experience within the bank. This implies a diverse mix of perspectives, with a balance between fresh insights and institutional knowledge, which could be beneficial in evaluating and enhancing internal control effectiveness in E-banking.

#### 4.2. Control environment of internal control systems

The second section of the questionnaire was intended to test the existence and the environment of the internal control system found in the organization. The control environment questions have included six interrelated points as discussed below;

##### 4.2.1. Integrity and ethical values related to E-banking

15% of the respondents strongly agree on the existence of a clear separation of roles and responsibilities in the bank, and 52% of the respondents agreed. 16% of the respondents are neutral and 15% and 1% of respondents are against the existence of separation of roles and responsibilities which are disagree and strongly disagree respectively. This result indicates that the bank has clear systems of integrity and ethical values related to E-banking.

Table 4.2.1 integrity and ethical values related to E-banking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	3	4.3	4.3	4.3
	Agree	46	65.7	65.7	70.0
	strongly agree	21	30.0	30.0	100.0
	Total	70	100.0	100.0	

Based on the provided data regarding the perception of integrity and ethical values related to E-banking, here's an interpretation:

- Strongly Agree (30.0%): A significant portion of respondents strongly agree that there is a clear separation of roles and responsibilities in the bank concerning E-banking. This indicates a high level of confidence and satisfaction among this group regarding the integrity and ethical values upheld in the bank's operations.
- Agree (65.7%): The majority of respondents agree with the existence of a clear separation of roles and responsibilities in E-banking. This further supports the notion that the bank has established systems to ensure integrity and ethical conduct in its E-banking practices.
- Neutral (4.3%): A small proportion of respondents are neutral, indicating that they neither agree nor disagree with the existence of separation of roles and responsibilities. This suggests some uncertainty or lack of strong opinion among this group.
- Disagree (1.4%): Combining the percentages of respondents who disagree and strongly disagree, it's evident that a very small minority (1.4%) are against the existence of a clear separation of roles and responsibilities in E-banking. While this is a minor dissenting opinion, Overall, the data suggests that the majority of respondents perceive the bank to have clear systems of integrity and ethical values related to E-banking, particularly regarding the separation of roles and responsibilities. However, it's important to consider and address the perspectives of those who are neutral or dissenting to ensure a comprehensive understanding of the bank's ethical practices.

#### 4.2.2. The development and performance of internal control related to E-banking

for the questions asked there are the development and performance of internal control related to E-banking 30% of the respondents strongly agreed, 48.6% of them were agreed, 21.4% were neutral as shown in the following table

Table 4.2.2 development and performance of internal control related to E-banking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	15	21.4	21.4	21.4
	Agree	34	48.6	48.6	70.0
	strongly agree	21	30.0	30.0	100.0
	Total	70	100.0	100.0	

- Strongly Agree (30%): This indicates a significant portion of respondents perceive the internal controls in E-banking to be highly effective. These respondents likely believe that the measures in place adequately safeguard against risks and ensure the security and integrity of e-banking transactions.
- Agree (48.6%): A majority of respondents agree that the internal controls in E-banking are effective. While not as emphatic as those who strongly agree, this still suggests a favorable perception of the controls' effectiveness. These respondents likely believe that the controls contribute positively to the security and reliability of e-banking services.
- Neutral (21.4%): A notable portion of respondents remain neutral, neither strongly agreeing nor disagreeing with the effectiveness of internal controls in E-banking. This could suggest uncertainty or lack of a clear opinion on the matter. It may indicate that these respondents require further information or experience to form a definitive judgment on the effectiveness of internal controls in E-banking. Overall, the data suggests a generally positive perception of the effectiveness of internal controls in E-banking, with a majority either strongly agreeing or agreeing. However, there is also a subset of respondents who remain neutral, indicating potential areas for improvement or further investigation to address any concerns or uncertainties.

#### 4.2.3. Reporting lines, and appropriate authorities and responsibilities

In the pursuit of objectives related to E-banking Out of all 70 respondents; only 27.1% strongly agreed on the existence of a specified reporting structure in the bank, 68.6% of the respondents agreed, and 4.3% were neutral. This result has indicated, the banks reporting structures have some inefficiencies/gaps as can be shown in the following table;

Table 4.2.3. Clear Structure of Reporting System

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	3	4.3	4.3	4.3
	Agree	48	68.6	68.6	72.9
	strongly agree	19	27.1	27.1	100.0
	Total	70	100.0	100.0	

#### 4.2.4. to attract, develop, and retain competent

individuals in alignment with objectives about E-banking 28.6% of the respondents strongly agreed that all E-banking products to attract, develop and retain competent 4.3% were neutral to respond to this question and there were equal percentage of responses 47.1% for agree and 20%disagree to attract, develop, and retain competent individuals in alignment with objectives pertaining E-banking.

Table 4.2.4. To attract develop and retain E-banking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	14	20.0	20.0	20.0
	Neutral	3	4.3	4.3	24.3
	Agree	33	47.1	47.1	71.4
	strongly agree	20	28.6	28.6	100.0
	Total	70	100.0	100.0	

Interpreting the data provided on the effectiveness of internal control in E-banking:

- Strongly Agree (28.6%): A significant portion of respondents strongly agree that E-banking products effectively attract, develop, and retain competent individuals in alignment with objectives. This indicates a strong belief that the strategies and initiatives related to E-banking are successful in attracting and retaining skilled individuals who contribute to achieving the objectives in this domain.
- Agree (47.1%): The majority of respondents agree that E-banking products effectively fulfill the objective of attracting, developing, and retaining competent individuals. While not as emphatic as those who strongly agree, this still suggests a positive perception of the effectiveness of E-banking strategies in talent management.
- Disagree (20%): A notable percentage of respondents disagree that E-banking products effectively serve the purpose of attracting, developing, and retaining competent individuals in alignment with objectives. This dissenting viewpoint suggests that there may be shortcomings or challenges in the current strategies or implementations related to talent management in the context of E-banking.
- Neutral (4.3%): A small portion of respondents remain neutral, neither agreeing nor disagreeing with the effectiveness of E-banking products in attracting, developing, and retaining competent individuals. This could indicate a lack of strong opinion or

uncertainty regarding the effectiveness of current practices in talent management within E-banking. Overall, the data suggests a mixed perception of the effectiveness of E-banking products in attracting, developing, and retaining competent individuals. While a significant portion agrees or strongly agrees, there is also a notable percentage that disagrees, indicating potential areas for improvement or further investigation to address any shortcomings or challenges in talent management within the E-banking sector.

#### 4.2.5. internal control responsibilities related to E-banking

for the hold's individuals accountable and responsibilities for their effectiveness internal control in E-banking. 34.3% of the respondents strongly agreed that the staff perform their operations based on the organization's procedures, 44% also agreed and 1.4% of the respondents were neutral. 8.6% of the respondents disagree and the rest 11.4% of the respondents are against as indicated in the following table. It shows that the majority of employees have good performance in their operations

Table 4.2.5 Individuals accountability and responsibility

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly disagree	8	11.4	11.4	11.4
	Disagree	6	8.6	8.6	20.0
	Neutral	1	1.4	1.4	21.4
	Agree	31	44.3	44.3	65.7
	strongly agree	24	34.3	34.3	100.0
	Total	70	100.0	100.0	

It seems that there is a high level of accountability perceived among respondents regarding internal control responsibilities related to E-banking. Here's an interpretation based on the provided data:

- **Strong Agreement on Accountability:** A significant proportion of respondents, 78.3% (34.3% strongly agree + 44% agree), expressed strong agreement that staff perform their operations based on the organization's procedures. This indicates a prevailing perception of accountability among employees regarding their internal control responsibilities in E-banking.
- **Minor Dissent:** While the majority of respondents expressed agreement, it's worth noting that 20% (8.6% disagree + 11.4% strongly disagree) of respondents disagreed with the statement. This suggests that there are still some concerns or discrepancies regarding perceived accountability, albeit from a smaller portion of respondents.
- **Minimal Neutral Response:** Only 1.4% of respondents were neutral, indicating a high level of certainty or agreement among the majority regarding staff accountability for internal control responsibilities.
- **Overall Positive Performance:** The data suggests a positive trend in employee performance within E-banking operations, with a notable majority aligning with organizational procedures. This is crucial for maintaining effective internal controls and mitigating risks associated with E-banking activities.
- **Areas for Improvement:** While the majority perception is positive, addressing concerns raised by the dissenting respondents can help identify specific areas for improvement within the internal control framework. Understanding their perspectives may reveal opportunities to enhance accountability mechanisms further. The data reflects a strong sense of accountability among employees for their internal control responsibilities in E-banking, with a notable majority aligning with organizational procedures. However, it's essential to address the concerns raised by dissenting respondents to ensure continuous improvement in internal control effectiveness.

### 4.3. Risk assessment of internal control systems

The third section of the questionnaire was intended to assess the strategy of identifying risks, an appropriate response to risks, management's role in identifying, evaluating, and responding to risks, and the occurrence of risks. The responses of the respondents are discussed below;

#### 4.3.1. the identification and assessment of risks relating to E-banking

This variable was intended to test whether the bank has designed an appropriate strategy for identifying risks. Out of which 40% and 50% of the respondents strongly agreed and agreed respectively that the strategy is designed appropriately, and 10% of the respondents were neutral. This shows that besides risk identification, appropriate responses for the identified risk are also essential tools in the risk assessment process the bank has a strategy that enables it to identify risks. The respondent's details have shown in the following table;

Table4.3.1. Strategy for Identifying Risks Effectiveness.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	7	10.0	10.0	10.0
	Agree	35	50.0	50.0	60.0
	Strongly agree	28	40.0	40.0	100.0
	Total	70	100.0	100.0	

#### 4.3.2. Objective achievement across the entity and analyzes risks

as a basis for determining how these risks should be managed, the majority of respondents have agreed that the bank has designed a system to offer appropriate responses to risks which is 21.4% and 65% of respondents strongly agree and agree respectively. 12.9% of the interviewed respondents are neutral to the raised questions. The bank's appropriate response rates for risks are to be managed but not as efficient as its vast as can be shown in the following tab

Table 4.3.2. Appropriate Response to Risks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	9	12.9	12.9	12.9
	Agree	46	65.7	65.7	78.6
	strongly agree	15	21.4	21.4	100.0
	Total	70	100.0	100.0	

It appears that there is a generally positive perception regarding the bank's ability to design a system for offering appropriate responses to risks. Here's an interpretation based on the data:

- **High Agreement on System Design:** The majority of respondents, totaling 86.4% (65.7% agree + 21.4% strongly agree), expressed agreement that the bank has designed a system to offer appropriate responses to risks. This indicates a prevailing perception that the bank has established mechanisms to address risks effectively.
- **Minimal Neutral Response:** Only 12.9% of respondents were neutral, suggesting that the majority of respondents had a clear opinion regarding the bank's risk response system. However, this neutral response might indicate some level of uncertainty or lack of information among a minority of respondents.
- **Efficiency Concerns:** While there is agreement that the bank has designed a system for responding to risks, the statement suggests that there may be concerns regarding the efficiency of these responses. This is implied by the statement, "not as efficient as its vast as can be shown in the following table."
- **Opportunity for Improvement:** The data highlights an opportunity for the bank to enhance the efficiency of its risk response mechanisms. While the system may be in place,

ensuring that responses are prompt, effective, and proportionate to the risks identified is essential for effective risk management.

- **Continuous Evaluation and Enhancement:** Addressing concerns related to the efficiency of risk responses requires ongoing evaluation and refinement of existing processes. By soliciting feedback from stakeholders and continuously monitoring risk performance, the bank can identify areas for improvement and implement necessary changes. While there is a positive perception regarding the bank's ability to design a system for responding to risks, there are concerns about the efficiency of these responses. By addressing these concerns and continuously improving its risk response mechanisms, the bank can enhance its overall risk management practices and better achieve its objectives across the entity.

#### 4.3.3. The potential for fraud in assessing risks related to the achievement of E-banking objectives.

The Majority of the respondents 61.4% have agreed and 25.7% of the respondents also strongly agreed that they consider the potential for fraud in assessing. Out of all respondents, 12.9% of They were neutral. The result indicates that management's role in identifying, evaluating, and responding to risk is high within the bank environment.

Table 4.3.3. consider the potential for fraud in assessing

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	9	12.9	12.9	12.9
	Agree	43	61.4	61.4	74.3
	Strongly agree	18	25.7	25.7	100.0
	Total	70	100.0	100.0	

There's a high level of acknowledgment and consideration of the potential for fraud in assessing risks related to the achievement of E-banking objectives within the bank environment. Here's an interpretation of the data:

- **Strong Agreement on Fraud Consideration:** A significant majority of respondents, comprising 87.1% (61.4% agree + 25.7% strongly agree), agreed that the bank considers the potential for fraud in assessing risks related to E-banking objectives. This indicates a strong recognition within the organization of the importance of addressing fraud risks in the context of E-banking operations.
- **Minimal Neutral Response:** Only 12.9% of respondents were neutral, suggesting that the vast majority of respondents had a clear stance regarding the consideration of fraud risks in risk assessment processes. This indicates a high level of awareness and understanding among employees regarding the importance of fraud prevention and mitigation measures.
- **Management's Role in Risk Management:** The data suggests that management plays a proactive role in identifying, evaluating, and responding to risks within the bank environment, particularly concerning fraud risks in E-banking. The high level of agreement among respondents reflects a strong organizational commitment to managing risks effectively.
- **Implications for Risk Management Practices:** The acknowledgment and consideration of fraud risks in risk assessment processes are essential for strengthening risk management practices within the bank. By actively addressing fraud risks, the bank can enhance its ability to protect against financial losses, safeguard customer information, and maintain trust and confidence in its E-banking services.
- **Continuous Vigilance:** While the data indicates a positive trend in terms of fraud risk consideration, it's crucial for the bank to maintain continuous vigilance and adaptability in response to emerging threats and evolving fraud schemes. Regular reviews and updates to risk assessment frameworks can help ensure that the bank remains resilient to potential

fraud risks over time. The data suggests that management within the bank environment recognizes the importance of considering the potential for fraud in assessing risks related to E-banking objectives. This proactive approach to risk management reflects a commitment to safeguarding the bank's interests and maintaining the integrity of its E-banking operations.

#### 4.3.4. The significant impact of the internal control for E-banking

61.4% of the respondents agreed on identifying and assessing changes that could significantly impact the internal control for E-banking, and 25.7% of the respondents also strongly agreed on it. Out of the respondents, 12.9% of them were neutral to respond for this variable

Table 4.3.4. impact the internal control for E-banking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	9	12.9	12.9	12.9
	Agree	43	61.4	61.4	74.3
	Strongly agree	18	25.7	25.7	100.0
	Total	70	100.0	100.0	

Based on the provided data on the effectiveness of internal control in E-banking, we can make the following analysis:

- **Overall Positive Perception:** The majority of respondents, comprising 87.1% (61.4% agree + 25.7% strongly agree), either agreed or strongly agreed with the effectiveness of internal control in E-banking. This indicates a prevalent positive perception among respondents regarding the efficacy of internal control measures within E-banking operations.
- **Minimal Neutral Response:** Only 12.9% of respondents were neutral, suggesting that the vast majority had a clear opinion about the effectiveness of internal control in E-banking.

While this neutral response indicates some level of uncertainty or lack of information among a minority of respondents, it's outweighed by the strong agreement expressed by the majority.

- **Strong Agreement on Effectiveness:** The data reflects a high level of agreement among respondents regarding the effectiveness of internal control in E-banking, with 87.1% expressing either agreement or strong agreement. This suggests a prevailing perception that internal control measures are robust and efficient in mitigating risks associated with E-banking activities.
- **Positive Implications for Risk Management:** The positive perception of internal control effectiveness bodes well for risk management practices within the E-banking domain. Effective internal controls are essential for safeguarding assets, ensuring data security, and maintaining regulatory compliance, all of which are critical aspects of risk management in E-banking.
- **Continued Monitoring and Improvement:** While the data indicates a positive perception of internal control effectiveness, it's essential for the organization to continue monitoring and improving its internal control processes over time. Regular assessments, audits, and updates to control mechanisms can help ensure that they remain aligned with evolving risks and regulatory requirements in the dynamic landscape of E-banking. The data suggests a strong vote of confidence in the effectiveness of internal control measures in E-banking, with the majority of respondents expressing agreement or strong agreement. This positive perception underscores the importance of robust internal control frameworks in mitigating risks and ensuring the integrity and security of E-banking operations.

#### 4.4. Control activities of internal control systems

The fourth section of the questionnaire was intended to assess the control activities and practices of internal control systems in the organization. It has been assessed. to the mitigation of risks

related to E-banking to acceptable levels, select and develop general control activities over technology to support the achievement of E-banking objectives, and deploy control activities through policies that establish what is expected and procedures that put policies related to E-banking into action to assess the bank's performance about the control activities discussed below as per the interviewed responses.

#### 4.4.1. To the mitigation of risks related to E-banking to acceptable levels

On the bank's performance of the internal control system of the bank, 52.9% of the respondents strongly agreed and 47.1% of the respondents agreed that the internal control system of the bank can reduce and detect fraud, misappropriations & other illegal activities. Since the banking sector is very sensitive to risks, the control environment should be strong enough. However, the bank's performance in the bank selection and development control activities contributes to the mitigation of risks related to E-banking to acceptable levels.

Table 4.4.1. to mitigate risks related to E-banking to acceptable levels

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	agree	33	47.1	47.1	47.1
	Strongly agree	37	52.9	52.9	100.0
	Total	70	100.0	100.0	

Based on the provided data, it appears that there is a positive perception among respondents regarding the bank's performance in terms of its internal control system's ability to mitigate risks related to E-banking to acceptable levels. Here's an analysis based on the table:

- **High Agreement on Risk Mitigation:** A significant majority of respondents, totaling 100% (52.9% strongly agree + 47.1% agree), expressed agreement that the internal control system of the bank can reduce and detect fraud, misappropriations, and other

illegal activities related to E-banking. This indicates a prevailing perception that the internal control mechanisms are effective in managing risks within acceptable levels.

- **Strong Confidence in Internal Controls:** The data reflects a high level of confidence in the internal control system's ability to address risks associated with E-banking activities. This suggests that the bank has implemented robust control activities aimed at mitigating fraud and other illegal activities, which are crucial in the sensitive banking sector.
- **Importance of Control Environment:** Given the sensitivity of the banking sector to risks, having a strong control environment is essential. The positive perception regarding the bank's internal control system indicates that it is performing well in selecting and developing control activities that contribute to risk mitigation in E-banking operations.
- **Continuous Improvement:** While the data indicates a positive perception of the bank's internal control system, it's important for the bank to continue monitoring and improving its control activities over time. Regular assessments, audits, and updates to control mechanisms can help ensure that they remain effective and aligned with the evolving risks in the E-banking landscape.
- **Commitment to Risk Management:** The high level of agreement among respondents underscores the bank's commitment to effective risk management in its E-banking operations. By investing in robust control measures, the bank can enhance its ability to safeguard assets, protect against fraud, and maintain regulatory compliance. The data suggests that there is strong confidence among respondents in the bank's internal control system's ability to mitigate risks related to E-banking to acceptable levels. This positive perception reflects the bank's proactive approach to risk management and its commitment to maintaining a strong control environment in the sensitive banking sector.

#### 4.4.2. General control activities over technology to support the achievement of E-banking objectives

Out of all respondents, 28.6% strongly agreed and 71.4% agreed that the banks to develop general control activities over technology to support the achievement of E-banking objectives.

specified in the following table; As shown in the result, the bank has selected and developed its internal control activities by technology by aligning the E-banking objectives

Table 4.4.2. selects and develops general control activities

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	agree	50	71.4	71.4	71.4
	strongly agree	20	28.6	28.6	100.0
	Total	70	100.0	100.0	

Based on the provided data, it is evident that there is a strong agreement among respondents regarding the bank's selection and development of general control activities over technology to support the achievement of E-banking objectives. Here's an analysis based on the table:

- **High Agreement on Technology Control Activities:** The majority of respondents, totaling 100% (71.4% agree + 28.6% strongly agree), expressed agreement that the bank has selected and developed general control activities over technology to support the achievement of E-banking objectives. This indicates a prevailing perception that the bank has effectively leveraged technology to enhance its internal control framework in the context of E-banking.
- **Alignment with E-banking Objectives:** The data suggests that the bank's internal control activities are aligned with its E-banking objectives. By utilizing technology-driven control measures, the bank is better positioned to address the unique risks and challenges associated with E-banking operations, such as cybersecurity threats and transaction processing efficiency.
- **Efficiency and Effectiveness:** Leveraging technology for internal control activities can enhance efficiency and effectiveness in risk management and compliance within the E-banking environment. Automation, data analytics, and real-time monitoring capabilities

enabled by technology can help detect and mitigate risks more proactively, thereby supporting the achievement of E-banking objectives.

- **Commitment to Innovation:** The high level of agreement among respondents reflects the bank's commitment to innovation and continuous improvement in its internal control practices. By embracing technological advancements, the bank demonstrates its proactive approach to adapting to evolving risks and regulatory requirements in the digital banking landscape.
- **Continuous Monitoring and Enhancement:** While the data indicates a positive perception of the bank's technology-driven control activities, the bank needs to continue monitoring and enhancing its technology infrastructure and control measures. Regular updates and assessments can help ensure that technology remains aligned with changing business needs and emerging risks in E-banking. The data suggests that the bank has effectively utilized technology to select and develop general control activities in support of its E-banking objectives. This proactive approach reflects the bank's commitment to leveraging innovative solutions to enhance its internal control framework and mitigate risks associated with E-banking operations.

#### 4.4.3. Deploys control activities through policies

that establish what is expected and procedures that put policies related to E-banking into action

The deploys control activities through policies that establish in the bank procedure has been strongly agreed and agreed by the respondents which is 45.7% and 42.9% respectively, 8.6% of the respondents were neutral and the rest 2.9% disagreed of this variable as shown in the following table. The result indicates that the bank has adopted accounting procedures that are segregated.

Table 4.4.3. deploys control activities through policies established by the bank procedures

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	disagree	2	2.9		2.9
	neutral	6	8.6	8.6	11.4
	agree	30	42.9	42.9	54.3
	Strongly agree	32	45.7	45.7	100.0
	Total	70	100.0	100.0	

Based on the provided data, it's evident that there is a strong agreement among respondents regarding the bank's deployment of control activities through policies and procedures related to E-banking. Here's an analysis based on the table:

- **High Agreement on Policy and Procedure Deployment:** The majority of respondents, totaling 88.6% (45.7% strongly agree + 42.9% agree), agreed that the bank deploys control activities through policies that establish expectations and procedures that put those policies related to E-banking into action. This indicates a prevailing perception that the bank has well-defined policies and procedures in place to govern E-banking activities and ensure compliance with established standards.
- **Minor Dissent:** While the majority of respondents agreed with the statement, it's worth noting that a small percentage (2.9%) disagreed, and 8.6% were neutral. However, the dissenting and neutral responses are relatively low compared to the overall agreement, suggesting a strong consensus among respondents regarding the effectiveness of the bank's policy and procedure deployment.
- **Segregation of Duties:** The statement also suggests that the bank has adopted accounting procedures that are segregated, which is a fundamental principle of internal control. Segregation of duties helps prevent fraud and errors by dividing responsibilities among different individuals to ensure checks and balances in financial processes.

- **Importance of Policies and Procedures:** Deploying control activities through well-defined policies and procedures is essential for maintaining transparency, consistency, and accountability in E-banking operations. Clear policies establish expectations, while procedures guide how to implement those policies effectively, reducing the risk of errors and irregularities.
- **Commitment to Compliance:** The high level of agreement among respondents reflects the bank's commitment to compliance and risk management. By adhering to established policies and procedures, the bank can mitigate risks associated with E-banking activities and ensure regulatory compliance. The data suggests that the bank has effectively deployed control activities through policies and procedures related to E-banking, with a strong consensus among respondents regarding the effectiveness of these measures. This indicates a proactive approach to internal control and risk management, which is crucial for maintaining trust and integrity in E-banking operations.

## 4.5. Information and communication

The fifth section of the questionnaire was intended to assess the information and communication practices of internal control systems in the organization. It has been assessed. or generates and uses relevant, quality information to support the functioning of internal control over E-banking, including objectives and responsibilities for internal control over E-banking, necessary to support the functioning of internal control specific to E-banking with external parties regarding matters affecting the functioning of internal control over and to E-banking into action to assess the bank's performance about the information and communication discussed below as per the interviewed.

#### 4.5.1. Relevant, quality information to support the functioning of internal control over E-banking.

In the bank how to generate and uses relevant, quality information related to effective internal control in E-banking

Table 4.5.1. relevant, quality information to support the functioning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	6	8.6	8.6	8.6
	Neutral	13	18.6	18.6	27.1
	Agree	33	47.1	47.1	74.3
	strongly agree	18	25.7	25.7	100.0
	Total	70	100.0	100.0	

Based on the provided data, it appears that there is a generally positive perception among respondents regarding the bank's generation and use of relevant, quality information to support effective internal control in E-banking. Here's an analysis based on the table:

- **High Agreement on Information Use:** The majority of respondents, totaling 72.8% (47.1% agree + 25.7% strongly agree), expressed agreement that the bank effectively generates and uses relevant, quality information to support internal control in E-banking. This indicates a prevailing perception that the bank has established processes for gathering and utilizing information that is essential for effective risk management and control in the E-banking domain.
- **Minimal Dissent:** While the majority of respondents agreed with the statement, a small percentage (8.6%) disagreed, and 18.6% were neutral. However, the dissenting and neutral responses are relatively low compared to the overall agreement, suggesting a

strong consensus among respondents regarding the bank's effectiveness in utilizing information for internal control purposes.

- **Importance of Information Quality:** The statement highlights the importance of relevant, quality information in supporting internal control activities. Utilizing accurate and timely information enables the bank to make informed decisions, identify emerging risks, and monitor the effectiveness of control measures in mitigating those risks.
- **Commitment to Data-driven Decision-making:** The high level of agreement among respondents reflects the bank's commitment to data-driven decision-making and risk management practices. By leveraging relevant, quality information, the bank can enhance its ability to anticipate and respond to challenges in the dynamic E-banking environment.
- **Continuous Improvement:** While the data suggests a positive perception of the bank's information usage for internal control, the bank needs to continue monitoring and enhancing its information management processes over time. Regular assessments and updates to data collection, analysis, and reporting mechanisms can help ensure that the information remains relevant, accurate, and aligned with evolving business needs and regulatory requirements. The data indicates a generally positive perception among respondents regarding the bank's generation and use of relevant, quality information to support effective internal control in E-banking. This suggests a strong foundation for data-driven decision-making and risk management practices within the bank's E-banking operations.

#### 4.5.2. To support the functioning of internal control specific to E-banking.

The bank internally communicates information, including objectives and responsibilities for internal control over E-banking, necessary to support the functioning of internal control specific to E-banking.

Table 4.5.2. support the functioning of internal control specific to E-banking.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	neutral	9	12.9	12.9	12.9
	agree	45	64.3	64.3	77.1
	Strongly agree	16	22.9	22.9	100.0
	Total	70	100.0	100.0	

Based on the provided data, it appears that there is a positive perception among respondents regarding the bank's internal communication of information, including objectives and responsibilities for internal control over E-banking.

- **High Agreement on Internal Communication:** The majority of respondents, totaling 87.2% (64.3% agree + 22.9% strongly agree), agreed that the bank internally communicates information necessary to support the functioning of internal control specific to E-banking. This indicates a prevailing perception that the bank effectively communicates objectives and responsibilities related to internal control in the context of E-banking operations.
- **Minimal Dissent:** While the majority of respondents agreed with the statement, a small percentage (12.9%) were neutral. However, the neutral responses are relatively low compared to the overall agreement, suggesting a strong consensus among respondents regarding the effectiveness of internal communication in supporting internal control activities specific to E-banking.
- **Importance of Clear Communication:** Effective internal communication is crucial for ensuring that all stakeholders understand their roles and responsibilities in maintaining internal controls over E-banking activities. Clear communication of objectives and responsibilities helps align efforts and ensures consistent adherence to control measures across the organization.

- **Support for E-banking Objectives:** The statement emphasizes the importance of aligning internal communication with the specific objectives and requirements of E-banking operations. By clearly communicating relevant information, the bank can enhance its ability to manage risks, maintain compliance, and achieve its E-banking objectives effectively.
- **Commitment to Transparency:** The high level of agreement among respondents reflects the bank's commitment to transparency and accountability in its internal control practices. By fostering open communication channels, the bank demonstrates its dedication to ensuring that all stakeholders are informed and empowered to contribute to the success of E-banking operations. The data indicates a generally positive perception among respondents regarding the bank's internal communication of information necessary to support internal control specific to E-banking. This suggests that the bank effectively communicates objectives and responsibilities related to internal control, contributing to the overall effectiveness of its E-banking operations.

#### 4.5.3. External parties regarding matters affecting the functioning of internal control over E-banking

How does the bank communicate with external parties regarding matters affecting the functioning of internal control over E-banking

Table 4.5.3. External parties regarding matters affecting the functioning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	disagree	2	2.9	2.9	2.9
	Neutral	3	4.3	4.3	7.1
	Agree	43	61.4	61.4	68.6
	strongly agree	22	31.4	31.4	100.0
	Total	70	100.0	100.0	

Based on the provided data, it appears that the bank effectively communicates with external parties regarding matters affecting the functioning of internal control over E-banking. Here's an analysis based on the table:

- **High Agreement on External Communication:** The majority of respondents, totaling 92.8% (61.4% agree + 31.4% strongly agree), expressed agreement that the bank communicates with external parties regarding matters affecting the functioning of internal control over E-banking. This indicates a prevailing perception that the bank actively engages with external stakeholders to ensure transparency and alignment of internal control practices with external requirements and expectations.
- **Minimal Dissent:** While the majority of respondents agreed with the statement, a small percentage (7.1%) were neutral or disagreed. However, the neutral and dissenting responses are relatively low compared to the overall agreement, suggesting a strong consensus among respondents regarding the effectiveness of external communication in addressing matters related to internal control over E-banking.

- **Importance of External Communication:** Effective communication with external parties, such as regulators, auditors, and other relevant stakeholders, is essential for ensuring that internal control practices align with industry standards, regulatory requirements, and best practices. By engaging with external parties, the bank can enhance its credibility, identify emerging risks, and demonstrate its commitment to transparency and accountability.
- **Compliance and Risk Management:** External communication plays a crucial role in compliance and risk management within the E-banking sector. By keeping external parties informed about internal control measures and practices, the bank can demonstrate its adherence to regulatory standards and its proactive approach to managing risks associated with E-banking operations.
- **Commitment to Transparency:** The high level of agreement among respondents reflects the bank's commitment to transparency and openness in its communication practices. By fostering effective communication channels with external parties, the bank demonstrates its dedication to maintaining trust and confidence in its E-banking operations. The data indicates a strong perception among respondents that the bank effectively communicates with external parties regarding matters affecting the functioning of internal control over E-banking. This suggests that the bank prioritizes transparency, compliance, and risk management by engaging with external stakeholders and aligning internal control practices with external expectations and requirements.

#### 4.6. Monitoring Activities

##### 4.6.1. the components of internal control related to E-banking are present and functioning

the bank selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control related to E-banking are present and functioning

Table 4.6.1. The component of internal control related to E-banking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	1	1.4	1.4	1.4
	Neutral	3	4.3	4.3	5.7
	Agree	45	64.3	64.3	70.0
	Strongly agree	21	30.0	30.0	100.0
	Total	70	100.0	100.0	

Based on the provided data, it appears that there is a strong perception among respondents that the bank selects, develops, and performs ongoing evaluations to ascertain whether the components of internal control related to E-banking are present and functioning. Here's an analysis based on the table:

- **High Agreement on Evaluation Practices:** The majority of respondents, totaling 94.3% (64.3% agree + 30.0% strongly agree), expressed agreement that the bank conducts ongoing evaluations to ascertain the presence and functioning of internal control components related to E-banking. This indicates a prevailing perception that the bank is proactive in assessing and monitoring the effectiveness of its internal control framework in the context of E-banking operations.

- **Minimal Dissent:** While the majority of respondents agreed with the statement, a small percentage (5.7%) were neutral or disagreed. However, the neutral and dissenting responses are relatively low compared to the overall agreement, suggesting a strong consensus among respondents regarding the bank's evaluation practices related to internal control in E-banking.
- **Importance of Ongoing Evaluation:** Continuous evaluation of internal control components is essential for identifying weaknesses, gaps, and areas for improvement within the control framework. By regularly assessing the presence and functioning of internal control components, the bank can enhance its ability to manage risks effectively and ensure compliance with regulatory requirements in the dynamic E-banking environment.
- **Commitment to Risk Management:** The high level of agreement among respondents reflects the bank's commitment to risk management and control effectiveness. By conducting ongoing evaluations, the bank demonstrates its proactive approach to identifying and addressing potential vulnerabilities and threats to E-banking operations.
- **Continuous Improvement:** Ongoing evaluations provide opportunities for continuous improvement and refinement of the internal control framework over time. By incorporating feedback from evaluations into decision-making processes, the bank can strengthen its internal control practices and adapt to evolving risks and challenges in the E-banking landscape. The data indicates a strong perception among respondents that the bank actively selects, develops, and performs ongoing evaluations to ascertain the presence and functioning of internal control components related to E-banking. This suggests that the bank is committed to maintaining a robust and effective internal control framework to support its E-banking operations.

#### 4.6.2. For taking corrective action

The bank evaluates and communicates E-banking internal control deficiencies on time to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Table 4.6.2. taking corrective action

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	1	1.4	1.4	1.4
	Neutral	1	1.4	1.4	2.9
	Agree	34	48.6	48.6	51.4
	Strongly agree	34	48.6	48.6	100.0
	Total	70	100.0	100.0	

Based on the provided data, it's evident that there is a strong agreement among respondents that the bank evaluates and communicates E-banking internal control deficiencies on time to the parties responsible for taking corrective action, including senior management and the board of directors.

- **High Agreement on Evaluation and Communication:** The majority of respondents, totaling 97.2% (48.6% agree + 48.6% strongly agree), expressed agreement that the bank evaluates and communicates E-banking internal control deficiencies promptly to the relevant parties responsible for corrective action, including senior management and the board of directors. This indicates a prevailing perception that the bank has established effective processes for identifying, assessing, and addressing internal control deficiencies in a timely manner.

- **Minimal Dissent:** While the majority of respondents agreed with the statement, a small percentage (3.6%) were neutral or disagreed. However, the neutral and dissenting responses are relatively low compared to the overall agreement, suggesting a strong consensus among respondents regarding the bank's practices related to evaluating and communicating internal control deficiencies in E-banking.
- **Importance of Timely Communication:** Prompt communication of internal control deficiencies is crucial for enabling timely corrective action and minimizing potential risks and impacts on E-banking operations. By promptly notifying senior management and the board of directors about identified deficiencies, the bank can ensure that appropriate measures are taken to address them and strengthen the overall control environment.
- **Commitment to Accountability:** The high level of agreement among respondents reflects the bank's commitment to accountability and transparency in its internal control practices. By effectively communicating internal control deficiencies, the bank demonstrates its dedication to proactive risk management and continuous improvement in E-banking operations.
- **Collaborative Approach to Corrective Action:** Involving senior management and the board of directors in the corrective action process ensures a collaborative approach to addressing internal control deficiencies. By engaging key stakeholders in decision-making and remediation efforts, the bank can enhance its ability to mitigate risks and strengthen its control framework over time. The data suggests a strong perception among respondents that the bank evaluates and communicates E-banking internal control deficiencies on time to the parties responsible for corrective action, including senior management and the board of directors. This indicates a proactive approach to risk management and a commitment to maintaining a robust internal control environment in E-banking operations.

## CHAPTER FIVE

### 5.1. Introduction

This chapter includes a summary of the study, conclusion, and recommendation as discussed below: -

### 5.2. Summary of the Study

Based on the analysis of the collected data, several key findings emerge regarding the demographic composition of respondents and their perspectives on internal control effectiveness in E-banking: The current position distribution indicates a hierarchical structure within the department, with different roles responsible for various aspects of internal control management, from operational oversight to strategic planning. This suggests a diverse sample, ensuring varied perspectives in the assessment of internal control effectiveness. However, efforts may be needed to further promote gender inclusivity. The predominance of middle-aged respondents indicates a mix of experienced individuals and potentially newer entrants into the workforce, providing a balance of perspectives. Other suggests a blend of fresh perspectives and moderate institutional knowledge among assessors, which could facilitate a comprehensive evaluation of internal control effectiveness. Overall, the data analysis highlights the diverse composition of respondents in terms of their roles, demographics, and experience levels. This diversity is beneficial for ensuring a holistic assessment of internal control effectiveness in E-banking, incorporating varied viewpoints and expertise to identify areas for improvement and enhance overall operational integrity and risk management.

The study assessed the internal control systems of a bank's e-banking division across various dimensions, including control environment, risk assessment, control activities, information communication and monitoring. The key findings and insights from each section is briefly summarized as follow.

- **Control Environment:** A significant majority of respondents perceived a clear separation of roles and responsibilities in the bank's e-banking operations, indicating strong integrity and ethical values. Most respondents agreed that the internal control system effectively supports the development and performance of e-banking operations. **Risk Assessment:**
- The majority of respondents recognized the importance of considering fraud risks in assessing risks related to e-banking objectives. There was a positive perception that the bank identifies and assesses changes that could significantly impact internal control for e-banking. **Control Activities:** Respondents strongly agreed that the internal control system can mitigate risks related to e-banking to acceptable levels, indicating confidence in the bank's risk management practices. There was strong agreement that the bank has selected and developed general control activities over technology to support the achievement of e-banking objectives. Most respondents agreed that the bank deploys control activities through policies and procedures effectively, ensuring transparency and compliance. **Information and Communication Practices:** The study indicates that the bank generates and utilizes relevant, quality information to support internal control in E-banking. Additionally, there is agreement among respondents that the bank effectively communicates objectives and responsibilities for internal control within the organization and with external parties. **Monitoring Activities Evaluation:** The majority of respondents believe that the bank actively monitors internal control components related to E-banking. There is strong agreement that the bank conducts ongoing evaluations to ascertain the presence and functioning of internal control components and communicates deficiencies promptly to relevant parties for corrective action. While the study highlights the bank's strengths in internal control, it also suggests areas for improvement. Recommendations include enhancing training programs, investing in advanced technology solutions, strengthening the segregation of duties, and fostering a culture of continuous improvement and collaboration among stakeholders.

### 5.3. Conclusion

The study provides valuable insights into the effectiveness of internal control systems within the context of E-banking operations. Based on the data analysis and interpretation, several key conclusions can be drawn: **Positive Perception of Internal Control Activities:** Overall, there is a positive perception among respondents regarding the bank's internal control activities related to E-banking. The majority of respondents agreed that the bank has implemented control activities to mitigate risks, select and develop technology-driven control measures, deploy policies and procedures, and communicate effectively with internal and external stakeholders. **Commitment to Risk Management and Compliance:** The study highlights the bank's commitment to risk management and compliance in its E-banking operations. Respondents indicated confidence in the bank's ability to detect and mitigate risks, align control activities with E-banking objectives, communicate effectively with stakeholders, and address internal control deficiencies on time. **Emphasis on Continuous Improvement:** While the study reflects positive perceptions of the bank's internal control systems, it also underscores the importance of continuous improvement. Recommendations include enhancing training programs, investing in advanced technology solutions, strengthening segregation of duties, and fostering a culture of transparency and accountability. **Collaborative Approach to Risk Mitigation:** The findings emphasize the importance of collaboration among internal and external stakeholders in mitigating risks associated with E-banking operations. Effective communication, timely evaluation of internal control deficiencies, and proactive corrective action involving senior management and the board of directors are essential for maintaining a robust control environment.

Overall, the study shows that the bank has established a strong foundation for managing risks and ensuring compliance in its E-banking operations. By implementing the recommended strategies for improvement and maintaining a proactive approach to risk management, the bank can further enhance the effectiveness of its internal control framework and ensure the integrity and reliability of its E-banking operations in an ever-changing landscape

#### 5.4. Recommendation of the study

Based on the conclusions drawn from the study, here are some recommendations for the bank's e-banking division to further strengthen its risk assessment practices:

In the control environment of internal control systems in the bank's e-banking division, the following recommendations can be made: Address inefficiencies or gaps in reporting structures by reviewing and possibly restructuring reporting lines and authorities. Clear and well-defined reporting structures ensure transparency, accountability, and effective oversight within the organization. Improve strategies for attracting, developing, and retaining competent individuals in alignment with objectives related to E-banking. This could involve implementing targeted recruitment efforts, providing ongoing training and development opportunities, and enhancing employee engagement initiatives. Regular training sessions and awareness programs to reinforce integrity, ethical values, and internal control principles among employees. This helps foster a culture of compliance and ethical conduct within the organization. Establish a system for continuous monitoring and evaluation of internal control mechanisms related to E-banking. This includes regular audits, risk assessments, and performance evaluations to identify weaknesses, gaps, or emerging risks and take proactive measures to address them. Foster an environment of open communication where employees feel comfortable raising concerns or reporting potential issues related to internal control. Implement channels for anonymous reporting to encourage whistleblowing and ensure timely resolution of issues. Leverage technology solutions to strengthen internal controls in E-banking operations. This could involve implementing advanced cybersecurity measures, automation of manual processes, and monitoring tools to detect and prevent fraudulent activities. Participate in industry benchmarking exercises and share best practices with peer organizations to stay abreast of emerging trends and adopt industry-leading practices in internal control management. Demonstrate strong leadership commitment to integrity, ethical conduct, and effective internal control management. Leaders should lead by example, communicate expectations clearly, and actively support initiatives aimed at enhancing internal control effectiveness.

In relation to risk, the bank sector was more sensitive to risk special CBE highly expansion and appropriate strategy to enhance Efficiency of Risk Response Mechanisms: The bank should focus on streamlining its processes for responding to identified risks. This may involve establishing clear protocols and escalation procedures to ensure timely and effective responses to emerging risks. Conduct regular training sessions and awareness programs for employees to enhance their understanding of risk assessment principles and fraud detection techniques. This will empower staff to proactively identify and mitigate risks in their day-to-day operations. Invest in advanced fraud detection and prevention technologies to strengthen the bank's defenses against evolving fraud schemes. Additionally, establish robust internal controls and monitoring mechanisms to detect and deter fraudulent activities effectively. Periodically review and update risk assessment frameworks to reflect changes in the e-banking landscape, regulatory requirements, and emerging threats. This ensures that risk assessment practices remain relevant and effective in mitigating current and future risks. Foster a culture of risk awareness and accountability across all levels of the organization. Encourage open communication and collaboration among employees to identify and address potential risks proactively. Recognize and reward individuals who demonstrate exemplary risk management practices. By implementing these recommendations, the bank can further enhance its risk assessment practices and strengthen its resilience against potential threats in the e-banking environment.

The same as to control activity the bank should Implement comprehensive training programs to ensure all employees are well-informed about the bank's internal control policies and procedures. This will help foster a culture of compliance and accountability throughout the organization. Conduct regular risk assessments to identify emerging threats and vulnerabilities in e-banking operations. This will enable the bank to proactively address potential risks and adapt its control measures accordingly. Continuously invest in advanced technology solutions to strengthen control activities and mitigate risks associated with e-banking. This may include implementing robust cybersecurity measures, enhancing fraud detection systems, and adopting innovative tools for monitoring and surveillance. Ensure that there is a clear segregation of duties within e-

banking operations to prevent potential fraud and errors. This can be achieved by establishing strict controls over access to sensitive information and transactional activities. Implement robust monitoring and reporting mechanisms to track the effectiveness of internal control measures and identify any deviations or anomalies in e-banking activities. This will enable timely intervention and corrective actions to mitigate risks. Conduct regular reviews and audits of the internal control systems to ensure compliance with regulatory requirements and industry best practices. This will help identify areas for improvement and strengthen the overall effectiveness of internal controls. Foster a culture of continuous improvement by encouraging feedback from employees and stakeholders regarding the effectiveness of internal control measures. Use this feedback to implement enhancements and optimizations to the control environment. Stay abreast of regulatory changes and industry trends related to e-banking operations. Ensure that internal control systems are updated accordingly to remain compliant with evolving regulatory standards. Foster collaboration with industry peers and regulatory bodies to share best practices and lessons learned in e-banking risk management and internal controls. This collaboration can provide valuable insights and help the bank stay ahead of emerging risks. Ensure active involvement and oversight from senior management in the implementation and monitoring of internal control systems. Senior management should demonstrate a strong commitment to risk management and provide the necessary resources and support to uphold a robust control environment.

Based on the findings of the study, depending on information communication and monitoring internal control framework some recommendations to further enhance the effectiveness of internal control systems within the context of E-banking operations: Given the importance of technology-driven control activities, the bank should continue to invest in advanced technological solutions such as artificial intelligence, machine learning, and data analytics. These tools can help improve fraud detection, transaction monitoring, and cybersecurity measures in E-banking operations. To ensure that employees are equipped with the necessary skills and knowledge to effectively implement internal control measures, the bank should enhance its training programs. Training should cover areas such as risk awareness, compliance with policies

and procedures, and emerging trends in E-banking security. Segregation of duties is essential for preventing fraud and errors in financial processes. The bank should review its current segregation of duties framework and identify any gaps or overlapping responsibilities. Clear delineation of roles and responsibilities can help enhance accountability and control effectiveness. Continuous improvement should be ingrained in the bank's organizational culture. Encourage employees to actively participate in identifying areas for enhancement, sharing best practices, and implementing innovative solutions to address emerging risks and challenges in E-banking operations. Effective communication and collaboration with external stakeholders such as regulators, auditors, and industry peers are crucial for staying abreast of regulatory developments and industry best practices. The bank should establish proactive channels for engagement with external parties to exchange information, share insights, and address mutual concerns related to E-banking. Policies and procedures related to internal control should be regularly reviewed and updated to reflect changes in regulatory requirements, technological advancements, and emerging risks in the E-banking landscape. Ensure that policies are documented, accessible to all relevant stakeholders, and aligned with the bank's strategic objectives.

By implementing these recommendations, the bank can strengthen its internal control framework, mitigate risks effectively, and maintain the integrity and reliability of its E-banking operations in an increasingly complex and dynamic environment. The bank can strengthen its internal control mechanisms, improve compliance with regulatory requirements, and enhance overall security and effectiveness in its e-banking operations.

As per the organization's significant role to the whole economy of the country as well as to the public sectors, taking corrective/appropriate actions should be absolute within the bank environment. This would ensure minimizing and protecting the bank's operations especially E-banking from future uncertainties.

## References

Amudo, A., and Inanga, L. (2009). Evaluation of Internal Control Systems: A Case Study from Uganda. International Research Journal of Finance and Economics.

Arens, Alvin A., Elder, Randal J., and Beasley, Mark S. (2012). Auditing and Assurance Services, Prentice Hall, USA.

Ayagre et al. (2014). The Effectiveness of Internal Control Systems of Banks: The Case of Ghanaian Banks, International Journal of Accounting and Financial Reporting, 4(2).

Bajaj, V., and Creswell, J. (2009). A Lender Failed, Did its Auditor? The New York Times, USA.

Committee of Sponsoring Organizations of the Treadway Commission (2013). Internal Control-Integrated Framework, USA.

Guidelines for Internal Control Standards (1992)

COSO (2013). Internal Control-Integrated Framework. New Jersey: COSO.

COSO, January 2009 (committee of sponsoring organizations of the tread way Commission); Internal Control-Integrated Framework, Introduction

COSO, September 2012; Internal Control-Integrated Framework; Committee of Sponsoring Organizations of the Tread Way Commission, Internal Control over External Financial Reporting: A Compendium of Approaches and Examples

Smith, J. (2020). Internal Controls in E-Banking: A Comprehensive Guide

( <https://www.mtu.edu>)

(Rokeya Sultana and Muhammad Enamul Haque, 2011).

QUESTIONNAIRE FOR RESEARCH PURPOSES  
ST. MARY UNIVERSITY  
SCHOOL OF GRADUATE STUDIES  
DEPARTMENT OF ACCOUNTING AND FINANCE

Dear respondents,

I'm a graduate student at St. Mary University in the Department of Accounting and Finance. Currently, I'm conducting research entitled "*Assessment of Internal Control Effectiveness in E-banking: In the Case of Commercial Bank of Ethiopia.*" as a partial requirement for the award of a Master's Degree in Accounting and Finance. The purpose of this questionnaire is to gather data for the proposed study. Therefore, you are kindly requested to assist in completing the study by providing the necessary information. I confirm that the information you share will stay confidential and only be used for academic purposes. Your honest response is vital for the study's success.

Thank you in advance for your kind cooperation.

Best Regards,

Meseret Bezabih

Part one: - Respondent Profile

1. What is your position currently?
2. Gender (Kindly tick appropriately where required)  
I. Female ☐ II. Male ☐

### 3. Age

I. 18 -35 []      II. 36 - 55 []      III. 56 & Above []

### 3. Work Experience

I. 1 to 5 years []      II. 5 to 10 Years []      III. More Than 10 Years []

## Part Two: - Measure the effectiveness of internal control in E-banking

### A: Control Environment

Item	Strongly disagree	disagree	Neutral	agree	Strongly agree
The bank demonstrates a commitment to integrity and ethical values related to E-banking					
The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control related to E-banking					
Management establishes board oversight structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives related to E-banking					
The bank demonstrates a commitment to attracting, developing, and retaining competent individuals in alignment with the objectives of E-banking					
The bank holds individuals accountable for their internal control responsibilities related to E-banking					

B: Risk Assessment

Item	Strongly disagree	disagree	Neutral	agree	Strongly agree
The bank specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to E-banking					
The bank identifies risks related to E-banking objective achievement across the entity and analyzes risks as a basis for determining how these risks should be managed					
The bank considers the potential for fraud in assessing risks related to the achievement of E-banking objectives.					
The bank identifies and assesses changes that could significantly impact the internal control for E-banking					

C: Control activities

Item	Strongly disagree	disagree	Neutral	agree	Strongly agree
The BANK selects and develops control activities that contribute to the mitigation of risks related to E-banking to acceptable levels					
The bank selects and develops general control activities over technology to support the achievement of E-banking objectives					
The bank deploys control activities through policies that establish what is expected and procedures that put policies related to E-banking into action					

D: Information and communication

Item	Strongly disagree	disagree	Neutral	agree	Strongly agree
The bank obtains or generates and uses relevant, quality information to support the functioning of internal control over E-banking.					
The bank internally communicates information, including objectives and responsibilities for internal control over E-banking, necessary to support the functioning of internal control specific to E-banking					
The bank communicates with external parties regarding matters affecting the functioning of internal control over E-banking					

E: Monitoring activities

Item	Strongly disagree	disagree	Neutral	agree	Strongly agree
The bank selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control related to E-banking are present and functioning					
The bank evaluates and communicates E-banking internal control deficiencies promptly to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.					