ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS AND ECONOMICS
DEPARTMENT OF ACCOUNTING AND FINANCE

Assessment of the Impact of the Effectiveness of Internal Control Systems on Fraud Prevention and Detection in Global Bank Ethiopia S.C

A Thesis Submitted to Department of Accounting and Finance in Partial Fulfillment of the Requirements for Master of Science Degree in Accounting and Finance

BY:

MASRESHA ENDALEW

ADVISOR:

DR. ALEM HAGOS (PHD)

JUNE, 2024
ADDIS ABABA, ETHIOPIA

Declaration

I affirm that this research is the original product of my independent and intellectual effort. No portion of this work has been previously submitted for a degree or any other qualification at this institution. While drawing upon the scholarly contributions of others for information and insight, all utilized sources have been meticulously referenced and acknowledged throughout the work.

Declared by:

Name: Masresha Endalew Tegegne

Signature: _____

Date: JUNE, 2024

Certification

I hereby certify that this research, undertaken under my direct and rigorous supervision, has been granted approval for submission to Accounting and Finance Department at AAU. This research satisfies a portion of the requirements for the award of the Master of Science (MSc) degree in Accounting and Finance.

Certified by:

Name: _____

Signature: _____

Date: _____

Addis Ababa University

Graduate school

This certifies that the research titled Effectiveness of Internal Control Systems on Fraud Prevention and Detection in Global Bank Ethiopia S.C, authored by Masresha Endalew Tegegne, fulfills a portion of the Master of Science (MSc) degree requirements in Accounting and Finance. The research adheres to University regulations and demonstrates originality and quality.

Examining Committee:

- Advisor:
    - Name: _____
    - Signature: _____
    - Date: _____
- Internal examiner:
    - Name: _____
    - Signature: _____
    - Date: _____
- External examiner:
    - Name: _____
    - Signature: _____
    - Date: _____

_____

Department Chair & Graduate Program Coordinator

JUNE, 2024

Addis Ababa, Ethiopia

Acknowledgments

The completion of this Master of Science (MSc) research in Accounting and Finance, titled "Effectiveness of (ICS) in Detecting and Preventing Fraud at Global Bank Ethiopia S.C.," owes its successful completion to the invaluable support and guidance I received.

I express my deepest gratitude goes to my advisor, Dr. Alem Hagos (PhD) for his exceptional guidance and mentorship during this research endeavor. His sharp insights, invaluable feedback, and constant encouragement were instrumental in shaping and strengthening my work.

My thanks also extend to Mr. Eshete Dametie for his significant contributions and support throughout the research. His openness in sharing his expertise and providing further insights proved immensely helpful in navigating challenges and maintaining the quality of my work.

My sincere thanks extend to all the participants who willingly shared their time and valuable insights through my questionnaire. Their contributions formed the bedrock of this research, and their rich data significantly deepened my understanding of the topic.

Finally, I acknowledge the divine providence of God throughout this endeavor. I am deeply grateful for the blessings of health, strength, and determination that sustained me on this journey, allowing me to see this research through to completion.

With heartfelt thanks to who have contributed to this research, I offer my profound gratitude. Your support and guidance have been instrumental in my success, and I am truly humbled by your generosity.

Table of Contents

List of Figure

List of Tables

Acronyms and abbreviation

AAU Addis Ababa University

ANOVA Analysis of Variance

CA Control Activity

CI Communication and Information

COSO Committee of Sponsoring Organization

EC Environmental Control

FPD Fraud Prevention & Detection

GBE Global Bank Ethiopia

ICS Internal Control System

MA Monitoring Activity

MFI Microfinance Institution

RA Risk Assessment

S.C Share Company

SBUs Sub-Business Units

SPSS Statistical Package for Social Science

Abstract

This research aimed to evaluate the effect of Global Bank Ethiopia's S.C (GBE) internal control system in deterring fraud. Specifically, the research investigated the primary causes of fraud within GBE, assessed the implementation of internal control mechanisms, and evaluated their success in detecting and preventing fraudulent activities. A structured questionnaire was used as a primary data collection instrument to select employees of GBE by purposive and convenient means. Items of the questionnaire were measured on the ranking scale. 57 employees from ten branches and audit department of the bank were sampled. The research investigated various components of GBE's internal control framework, including the control environment, risk assessment procedures, implemented control activities, information flow and communication protocols, and monitoring practices. Data analysis was done using descriptive and inferential statistics. The research found that employees of the bank perceived that; poor internal control system, presence of unqualified staff, inadequate staffing, poor record-keeping practices, and inadequate training and re-training of staff among others were the main causes of fraud. All aspects of internal control system were strongly implemented and practiced by the bank. Internal control system was effective in controlling fraud in the bank in various forms. Fraud had negative and insignificant effect on the performance of the bank. The research recommends the continuous practice of the internal control system to ensure that fraud of any form is reduced to the barest minimum.

Keywords: *Internal control systems, fraud prevention and detection, internal control components,*

CHAPTER ONE

Background of the research and organization

1.1 Introduction

The banking industry, entrusted with safeguarding vast financial resources, operates in a landscape brimming with complex operations and inherent vulnerabilities. This underscores the crucial role of robust internal control systems (ICS) in mitigating the ever-present threat of fraud. This chapter delves into the critical domain of ICS efficacy specifically within the context of Global Bank Ethiopia S.C a key player in the Ethiopian financial landscape.

Through a comprehensive exploration of theoretical and empirical frameworks, this chapter dissects the intricate relationship between ICS design, implementation, and the prevention and detection of fraudulent actions within banking institutions. The discussion revolves around key elements of ICS, including the control environment, risk assessment procedures, control activities, information and communication channels, and ongoing monitoring mechanisms. By analyzing their interconnectivity and impact on fraud mitigation, the chapter establishes a foundational understanding of ICS functionality within the banking environment.

Furthermore, the chapter focuses on the specific case of Global Bank Ethiopia S.C. Employing a blend of theoretical frameworks and practical insights gleaned from within the bank; the chapter assesses the effectively of the implemented ICS in preventing and detecting fraud. This analysis delves into the specific internal control techniques employed by Global Bank Ethiopia S.C, their alignment with industry best practices, and their efficacy in addressing the unique risk landscape faced by the bank. This nuanced examination sheds light on the strengths and weaknesses of the existing ICS, paving the way for potential recommendations and improvements.

Moving beyond the confines of Global Bank Ethiopia S.C, the chapter also touches upon the broader importance of this research for the Ethiopian banking industry as a whole. By

establishing a framework for evaluating ICS effectiveness, the research has the potential to guide other banks in strengthening their defenses against fraud, ultimately fostering a more secure and trustworthy financial ecosystem within Ethiopia.

Ethiopia's burgeoning economy relies heavily on a stable and secure banking sector to foster growth and development (World Bank, 2023). Banks act as the lifeblood of the financial system, channeling resources, facilitating transactions, and ultimately boosting economic activity. Yet, as demonstrated by financial crises around the world, the stability and trust within the banking sector hinge on robust internal control systems (Adams, C. E., & McNair, M. S., 2018). These systems serving as the primary safeguard against fraud, preserving financial resources and ensuring the reliability of financial reporting.

Banking institutions hold a significant role within the financial system of nations, playing a crucial part in the economic development process (McKinsey & Company., 2016). They act as intermediaries between surplus and deficit units, contributing to the overall increase in national savings and investments, consequently boosting the nation's output (Levine, 1991). Additionally, banks possess the power to create money by providing credit, directly impacting the money supply level. This, in turn, has a profound effect on the development of national income, as it dictates the extent of economic activity within a nation (Mishkin, 2007).

Banks play a pivotal role in the payments system, enabling smooth economic dealings among diverse national and international economic entities. In doing so, they actively foster and advance trade, commerce, and industry (Beck, T., & Levine, R., 2004).

In order for banks to operate efficiently and make significant contributions to a nation's development, it is imperative that the industry remains stable, secure, and reliable. To achieve these necessary conditions, the establishment of a robust accounting system is crucial, which is facilitated by an internal control system (Adams, C. E., & McNair, M. S., 2018). An effective framework of internal controls serves as an essential component of bank management and serves as the bedrock for the secure and trustworthy functioning of banking sectors (Institute of Internal Auditors., 2023). It is worth noting that

inadequate or inefficient internal controls have been responsible for financial losses in numerous banks and have played a function in the collapse of banking organizations worldwide (Watts, R. L., & Zimmerman, J. L., 1986).

As per the guidelines provided by the International Organization of the Supreme Audit Institutions (INTOSAI, 2001), internal control is a comprehensive process influenced by both the management and personnel of an organization. Its purpose is to mitigate risks and offer a reasonable level of assurance in achieving the organization's mission.

The establishment, evaluation, and supervision of efficient internal control systems play a crucial role in determining the quality of financial reporting. Precisely, robust internal controls minimize the deliberate manipulation of information provided to external parties, diminish the likelihood of accidental procedural and estimation errors in reporting, and alleviate the inherent risks associated with business operations (Kinney, 2000).

Based on the preceding analysis, it is evident that internal control holds significant importance in ensuring the smooth functioning of businesses. The objective of this research is to examine the role of internal control systems in protecting assets from fraudulent activities within the Ethiopian banking sector, with a specific focus on the case of Global Bank Ethiopia S.C.

Within the Ethiopian banking landscape, understanding the effectiveness of internal controls takes on particular significance due to the industry's rapid growth and evolving regulatory environment. As a prominent player in this landscape, Global Bank Ethiopia S.C presents a compelling case study to investigate the interplay between internal controls and fraud prevention. This research aims to delve into the specific measures implemented by Global Bank Ethiopia S.C, assess their efficacy in mitigating fraud risks, and ultimately shed light on their impact on the bank's financial health and operational efficiency.

Established in August 2012 as Debub Global Bank S.C. and later renamed Global Bank Ethiopia S.C., this privately owned bank has carved a prominent space in the Ethiopian

banking landscape. Starting with a subscribed capital of Birr 266.9 million and paid-up capital of Birr 138.9 million, it has witnessed impressive growth over the past decade. As of today, its subscribed capital stands at Birr 3 billion, while its paid-up capital has increased to Birr 700 million. This upward trajectory is further reflected in its expanding branch network, ballooning from 15 to a remarkable 200 branches across the capital and regional cities, serving over 450,000 satisfied customers nationwide. The bank's total assets have also impressively crossed the Birr 4 billion mark.

This remarkable success can be attributed to the dedication and collaborative efforts of its loyal customers, committed employees, supportive shareholders, and engaged stakeholders. These stakeholders are the driving force behind Global Bank Ethiopia's S.C diverse scope of domestic and foreign banking services, delivered with a focus on superior customer service standards.

In conclusion, this introductory chapter establishes the rationale for analysis the effectiveness of internal control systems in preventing and detecting fraud at Global Bank Ethiopia S.C. By highlighting the importance of robust ICS and its impact on the broader banking industry, it sets the stage for a comprehensive analysis of the bank's internal control landscape, paving the way for valuable insights and actionable recommendations.

1.1 Statement of the Problem

The past decade has witnessed a surge of academic and professional interest in internal control systems, primarily fueled by a wave of international financial scandals. Researchers have dedicated significant effort to researching the effectiveness and efficiency of control frameworks implemented in both private and public sectors, often prescribed by relevant authorities (Smith, 2023).

Modern research delves deeper, analyzing the consequence of adhesion and non-adhesion to internal controls on organizational outcomes ((COSO)., 2013). COSO's five key components – control environment, risk assessment, control activities, information and

communication, and monitoring activity – form the foundation for understanding how internal controls influence an entity's goals and objectives.

While a substantial body of research exists (dating back over a decade), many researches focus on broader aspects of internal control or utilize outdated methodologies. Examples include Brewer and List's (Geiger, 2004) work on measuring system effectiveness and research on assessing controls in Nigerian government ministries. Similarly, (Douglas, 2011) research on internal control and financial management in Ghanaian public sectors falls into this category.

However, the dynamic nature of our society demands continuous investigation to capture evolving complexities. Recognizing this gap, this research ventures into uncharted territory by specifically focusing on internal control activities. As the core building blocks of the system, understanding their influence on financial management, particularly in the public sector, holds immense significance.

Research on the relationship between internal controls and fraud prevention in banks presents a mixed picture. For instance, (Fikru Worku., 2018) found a positive correlation in Ethiopia, while Leah N. & Dr. Josiah A. (IIA, 2017) reported a negative relationship in Kenyan banks. (Idowu, S. O., & Adedoku, A. O., 2013), from Nigeria also concluded a positive association between robust control systems and fraud mitigation. These discrepancies highlight the need for further exploration, especially in Ethiopia, where research on this topic remains scarce. Existing researches often suffer from limitations such as descriptive or correlational research designs, which fall short of establishing causality. Additionally, insufficient sample sizes and inconsistent methodologies contribute to conflicting findings.

This research aims to bridge these gaps by employing a stratify approach specifically focused on Global Bank Ethiopia S.C. By analyzing the sample population of relevant data within the bank, the research achieves greater confidence in the findings. Furthermore, the research adopts an explanatory research design to delve deeper into the causal correlation between internal control activities and fraud prevention and detection.

By combining a comprehensive sample with a robust methodology, this research strives to deliver reliable and insightful conclusions regarding the effectiveness of Global Bank Ethiopia's S.C internal control systems in preventing fraud. The primary research question driving this investigation is: "To what extent do the internal control activities designed and implemented by Global Bank Ethiopia S.C. contribute to the prevention and detection of fraudulent actions within the bank?"

1.2 Research Questions

This research investigated the effectiveness of internal controls at Global Bank Ethiopia S.C in preventing and detecting fraud. The research addressed key questions that emerged during the research process, aiming to solve problems related to FPD.

- Are the five components of the internal control system (control environment, risk assessment, control activities, information and communication, and monitoring activity) effective in Global Bank Ethiopia S.C?
- Do specific components of the COSO framework demonstrate greater effectiveness in fraud prevention and detection compared to others within Global Bank Ethiopia S.C?
- Does the effectiveness of Global Bank Ethiopia's S.C ICS enhance the leadership capabilities of the organization and operational efficiency of the bank?
- How does the strength of the bank's internal control system correlate with its ability to prevent and detect fraudulent activities?
- Can specific internal control activities implemented by Global Bank Ethiopia S.C effectively identify and "fish-out" individuals or groups involved in fraudulent activities within the bank?
- Is there a dedicated strategy employed by Global Bank Ethiopia S.C to detect and identify fraud incidents arising from human factors such as a combination of inattention, tiredness, and misunderstandings
- How does Global Bank Ethiopia S.C adapt and refine its ICS based on emerging fraud risks and evolving technologies within the banking industry?

1.3 Objectives of The Research

1.4.1 General Objective:

To comprehensively assess the effectiveness of internal control system employed by Global Bank Ethiopia S.C. in preventing and detecting fraudulent activities within the bank.

1.4.2 Specific Objectives:

- Identify and evaluate the effectiveness of specific internal control components and activities implemented by Global Bank Ethiopia S.C, based on the COSO framework, in preventing and detecting fraud.
- Analyze the relationship between the efficiency of internal control techniques and the bank's ability to detect and deter fraudulent activities.
- Assess the effectiveness of existing internal control measures in mitigating specific types of fraud commonly encountered within the Ethiopian banking sector.
- Evaluate the sufficiency of the bank's response mechanisms to internal control findings and recommendations, focusing on how these actions address identified vulnerabilities and prevent future fraud occurrences.
- Investigate the effectiveness of the bank's monitoring activities in controlling the ongoing effectiveness and adaptation of its internal control system in response to evolving fraud risks and industry changes.

1.4 Hypothesis

The COSO framework emphasizes that the control environment fits the timber for an entity's control activities (COSO, 2013). A strong ethical culture discourages fraudulent behavior, while management commitment and clear communication of control policies ensure employees realize their functions and responsibilities in upholding the internal control system (COSO, 2013). This collectively creates a more robust environment that hinders fraudulent activities and empowers employees to identify and report suspicious behavior.

Ha1: There is a significant relationship between control environment and fraud control in Global Bank Ethiopia.

The COSO framework highlights the importance of risk assessment in identifying potential threats to financial reporting and control objectives (COSO, 2013). By proactively identifying and prioritizing fraud risks specific to the Ethiopian banking sector, the bank can tailor its control activities to address those specific vulnerabilities (COSO, 2013). This targeted approach allows for a more effective mitigation strategy against relevant fraud threats.

Ha2: There is a significant relationship between risk assessment and fraud control in Global Bank Ethiopia.

Control activities are the procedures and policies implemented to reference identified risks (COSO, 2013). According to COSO, well-designed and implemented control activities directly impact the effectiveness of the ICS (COSO, 2013). By aligning control activities with specific fraud risks, the bank can directly prevent or detect fraudulent attempts (COSO, 2013). This reduces the bank's overall exposure to financial losses and reputational damage.

Ha3: There is a significant relationship between control activity and fraud control in Global Bank Ethiopia.

The COSO framework emphasizes the importance of communication in ensuring employees realize their functions in the internal control system (COSO, 2013). When control policies, procedures, and fraud risks are effectively communicated across all levels, employees become more aware of their accountabilities and empowered to identify potentially fraudulent activities (COSO, 2013). This improved awareness directly leads to better fraud detection within the bank (COSO, 2013).

Ha4: There is a significant relationship between information and communication and fraud control in Global Bank Ethiopia.

Monitoring is a crucial component of the COSO framework as it ensures the ongoing effectiveness of the internal control system (COSO, 2013). Regular and independent monitoring activities allow the bank to identify any weaknesses in the system, particularly in response to evolving fraud risks (COSO, 2013). By promptly addressing these weaknesses, the bank can prevent future fraudulent activities and maintain a strong internal control environment (COSO, 2013).

Ha5: There is a significant relationship between monitoring activity and fraud control in Global Bank Ethiopia.

1.5 Significance of The Research

Assessing the effectiveness of Global Bank Ethiopia S.C.'s internal control system is crucial for several reasons:

Reduced Fraud Risk: Strong control systems minimize fraudulent activity, fostering a safer and more ethical work environment. This can contribute to increased job satisfaction and a preference for working in a bank with a strong ethical foundation. Enhanced Risk Management: A robust control framework helps the bank identify and mitigate risks associated with operations. By understanding these risks, employees can make informed decisions and perform their duties with greater confidence**.** This empowers them with the knowledge necessary to contribute to the bank's overall risk management strategy. Improved Regulatory Compliance: Effective internal controls ensure adherence to regulations, minimizing legal risks and reputational damage for the bank. This reduces stress and uncertainty for employees who may otherwise be concerned about potential regulatory violations. Knowledge of the regulations and how internal controls address them allows for a more compliant and secure work environment. Strengthened Stakeholder Confidence: Demonstrating robust control systems fosters trust amongst customers, investors, and regulators. This can lead to increased job security for employees as the bank's stability strengthens. Additionally, a strong reputation attracts and retains top talent who might have a preference for working in a well-regarded organization. Best Practices and Benchmarking: The research’s findings can provide

valuable insights and best practices for other banks in Ethiopia. This fosters a knowledge-sharing environment within the industry, promoting continuous improvement in fraud prevention across the sector. Employees benefit from working in a bank that actively seeks knowledge advancement and implements best practices. Tailored Control Models: Understanding the specific effectiveness of different control components can guide other banks in tailoring their systems. This knowledge transfer can empower employees in other institutions to advocate for control enhancements based on proven effectiveness. Adapting to Technological Advancements: The research can shed light on how control systems need to adapt to emerging fraud risks associated with new technologies. This knowledge allows the bank to equip employees with the skills and training necessary to identify and address these evolving threats. Employees benefit from having the tools and knowledge to stay ahead of emerging risks in a dynamic technological landscape. Building a Culture of Integrity: By analyzing employee perceptions and control environment effectiveness, the research can contribute to fostering a culture of ethical conduct and vigilance within the bank. Understanding employee preferences for ethical practices allows the bank to tailor control systems and training programs to cultivate a strong moral compass and a zero-tolerance approach to fraud. This can significantly enhance employee morale and job satisfaction.

In conclusion, assessing Global Bank Ethiopia's S.C internal control system goes beyond just regulatory compliance. It directly impacts employee preferences for a safe and ethical work environment, empowers them with knowledge for informed decision-making, and promotes continuous learning within the organization.

1.6 Scope of the Research

1.7.1 Geographical Scope

The geographical range of this research encompasses two locations in Addis Ababa: the Head Office and branches within the East District. The Head Office serves as the central hub for internal control systems, allowing for an in-depth analysis of their design and implementation across various departments. This focus on the Head Office provides a baseline understanding of the bank's overall control framework.

In contrast, the inclusion of branches within the East District enables a comparison of control mechanisms at the individual branch level. This comparison will investigate potential variations in effectiveness between the central systems and their application at individual branches, offering valuable insights for improving fraud prevention efforts across the organization.

1.7.2 Conceptual Scope

The conceptual scope of this research draws upon the COSO internal control framework, examining its five components in relation to fraud prevention and detection at Global Bank Ethiopia S.C. Specifically, the research was analyze:

Banks rely on a layered internal control system to combat fraud. This system starts with a strong leadership that emphasizes honesty and ethical behavior, along with ways for employees to report suspicious activity. Then, the bank identifies and analyzes areas vulnerable to fraud within different departments. To address these risks, they implement specific policies and procedures, like controlling transactions, separating employee duties, and restricting access to sensitive information. Clear communication channels ensure everyone is aware of fraud risks and how to report them. Finally, the bank regularly assesses how well these controls work and makes adjustments as needed.

By analyzing these interconnected elements within the COSO framework, the research investigates the following key questions...

- How well does each part of Global Bank's internal control system prevent and catch fraud?
- What are the good and bad points of the current system for stopping fraud?
- What can Global Bank do to improve its internal controls and make fraud even less likely?

1.7.3 Time Scope

The research on the effectiveness of internal control systems in preventing and detecting fraud was conducted within a seven-month timeframe, with data collection primarily focused on September and October 2023. This period was chosen to capture insights during the peak financial season for Global Bank Ethiopia S.C., while acknowledging that the analysis of fraud occurrence and control system effectiveness were consider data and historical trends from a broader timeframe extending beyond the three months of data collection.

While there could be potential limitations associated with focusing on a specific period, such as seasonal variations in fraud activity, the collected data was analyzed within the context of the bank's overall internal control systems and long-term fraud prevention efforts.

1.7 Limitation of the Research

This research, like any research endeavor, has certain limitations. The sample size consisted of only 57 participants, including 4 directors, 23 managers, 15 senior auditors, at the Head Office of Global Bank Ethiopia S.C and 15 branch officers. While focusing on one bank allowed for an in-depth analysis of its internal control systems, it necessarily limits the generalizability of the findings to other banks or the wider Ethiopian banking industry. Additionally, certain factors specific to Global Bank Ethiopia S.C, such as its size, internal culture, and regulatory environment, could influence the applicability of the findings to other contexts.

Furthermore, relying solely on quantitative data gathering methods like surveys and document reviews might have limited the depth of understanding of the complex interplay between internal control systems and fraud prevention. Qualitative methods like interviews could have provided richer insights into employee perceptions, cultural nuances, and informal control mechanisms that quantitative data might miss.

However, the use of a mixed-methods approach helps mitigate these limitations. By combining quantitative data on the effectiveness of control components with qualitative insights from interviews with key stakeholders, the research can achieve a more holistic understanding of the dynamics of fraud prevention within Global Bank Ethiopia S.C. This allows for a more robust and comprehensive research that captures both the measurable aspects of control systems and the contextual factors that influence their effectiveness.

1.9. Organization of the Research

The five-chapter research paper begins with an introduction that establishes the research's context, problem, questions, hypothesis, objectives, significance, scope and limitation. The following chapter dives into the existing literature surrounding the research area. The third chapter details the methodology, including the research approach, data sources, sampling techniques, and data gathering and analysis methods. Chapter four analyzes, discusses, and interprets the collected data. Finally, the concluding chapter summarizes the key findings, offers recommendations, and provides references.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction:

The Ethiopian banking sector has witnessed immense growth in recent years, driven by economic liberalization and financial deepening. However, this rapid expansion has also been accompanied by increasing concerns about fraud. To mitigate these risks, robust internal control system (ICS) plays a crucial function in safeguarding assets and deterring fraudulent activities. This literature review examines the effectiveness of ICS in preventing and detecting fraud specifically within the context of Global Bank Ethiopia S.C, a prominent player in the Ethiopian banking landscape.

Ethiopia's booming banking sector, fueled by economic reforms and financial inclusion, faces a growing challenge: fraud. Strong internal controls (ICS) are essential for Global Bank Ethiopia S.C., a key player in this dynamic market, to protect its assets and deter fraudulent activity. This review explores the effectiveness of ICS in preventing and detecting fraud within the specific context of Global Bank Ethiopia S.C.

2.2 Theoretical Review:

2.2.1 Internal Control Frameworks:

Several frameworks exist to guide the plan and execution of internal control systems (ICS). Preeminent among these is the COSO Internal Control Framework, which identifies five interrelated elements: control environment, risk assessment, control activities, information and communication, and monitoring activities ((COSO)., 2013). These components form the cornerstone for understanding how ICS impacts an organization's power to accomplish its goals, including fraud prevention and detection.

2.2.2 Internal Control System Concepts:

An organization's internal control system (ICS) refers to the interconnected policies, procedures, and processes it implements. These controls aim to achieve several objectives: protecting assets, ensuring reliable financial records, promoting operational efficiency, and adhering to applicable laws and regulations (David Ingram, 2019). A well-designed ICS is particularly critical in the financial sector, where it acts as a vital line of defense against fraudulent activities (David Ingram, 2019).

Controls are implemented to provide confidence in an organization's operations, reporting, and legal adherence. This research focuses on internal controls, a system designed to manage these aspects. Internal control definitions vary due to stakeholder and level of impact. (Millichamp A. H., 2002), defines it as a comprehensive system, including financial controls, established by management to ensure organized and efficient operations, policy adherence, asset protection, and record accuracy. The widely adopted COSO framework specify it as a procedure implemented by various levels of an organization to supply reasonable assurance of achieving goals in effectiveness, efficiency, reliable financial reporting, and legal compliance ((COSO)., 2013).

This system of checks and balances helps make sure operations run smoothly, finances are reported accurately, and the entire rules are followed. There are two main types of controls, internal and external. This research will only look at internal controls. Internal control has various definitions as it impacts different stakeholders of an organization in different ways and at different levels. According to (Millichamp A. , 2002), internal control refers to a comprehensive system of controls, including financial controls, established by management to conduct business in an organized and efficient manner, ensure adherence to management policies, protect assets, and ensure the completeness and accuracy of records. COSO, a respected framework in the US, defines internal controls as a system managed by a company’s leadership and staff. This system helps ensure the company meets its goals in three areas: efficient operations, trustworthy financial reporting, and following regulations.

Organizations implement internal controls, a set of policies and procedures, to ensure they achieve their goals and objectives (Rezaee, 2002). These controls guarantee that transactions are processed correctly to prevent waste, theft, and misuse of resources. Internal control systems also contribute to efficient performance, resource protection, reliable reporting, and legal compliance. In essence, management establishes internal controls to ensure the organization operates in an orderly and efficient manner, adhering to policies, safeguarding assets, and maintaining accurate records.

2.2.3 Establishment of Internal Control System:

Every business relies on an accounting system to process transactions and maintain historical records (Attwood, F. A. & Stein, N. D., 1986). Complementing this, management has a responsibility to establish an internal control system (ICS), either independently or with the help of external consultants, internal audit, or accounting personnel (Millichamp, A.H., 2002). This duty stems from management's fiduciary obligation to operate the business efficiently, ensure adherence to internal policies, safeguard assets, and guarantee the accuracy and completeness of financial records. It's important to note that ICS design should be tailored to management's specific needs. However, the input of the internal audit department, with their expertise in evaluating the potential impact of control systems, is invaluable for establishing effective internal controls.

2.2.4 Objectives of Internal Controls:

Recent years have seen a growing focus on internal control methods, driven by both the increasing complexity of business practices and the expansion of business units (Howard, 1984). Howard argues that these methods not only enhance efficiency but also act as safeguards against errors and fraud. Effective internal controls must meet specific objectives to ensure both accuracy and efficiency, thus providing reasonable assurance. These objectives include:

- Validity of transactions: The system should prevent recording fictitious or nonexistent transactions (Howard, 1984).
- Proper authorization: The system should ensure transactions have proper authorization (Howard, 1984).
- Completeness of recording: Procedures should prevent omitting transactions from the records (Howard, 1984).
- Accurate valuation: The system should include measures to avoid errors in calculating and recording transactions at any stage (Howard, 1984).
- Correct classification: The system should ensure transactions are categorized appropriately (Howard, 1984).
- Timely recording: Effective controls should ensure transactions are recorded at the correct time to avoid omissions or inaccuracies (Howard, 1984).

2.2.5 Types of Internal Control Systems:

Internal control frameworks typically categorize controls into preventive, detective, and corrective types (Millichamp A. H., 2002). However, variations exist in these classifications (Millichamp A. H., 2002). (Millichamp A. H., 2002), emphasizes controls that focus on safeguarding assets, separating duties, and ensuring proper supervision, verification, approval, and authorization processes, alongside robust documentation and reporting. Other sources, such as (Lousteau, 2006), the State University of New York, and (Dinapoli, 2005), utilize a more comprehensive classification scheme that encompasses directive controls, preventive controls, compensating controls, detective controls, and corrective actions.

2.2.5.1 Preventive Control:

Preventive controls, as described by (Lacotelli, 2009), are proactive measures implemented by management to prevent deviations from established directives, policies, and procedures. These controls aim to reduce the likelihood of errors, fraud, and irregularities in transactions, ultimately protecting the organization from potential losses

(Lacotelli, 2009). Examples include segregation of duties, well-defined authorization and approval processes, clear organizational structures outlining responsibilities, thorough documentation, physical security measures for assets, and ongoing employee training.

2.2.5.2 Detective Controls:

While preventive controls are ideal, detective controls play a crucial role in uncovering errors, fraud, and irregularities after they occur (Wells, 2006). These controls, such as post-audits, exception reports, and validation, detect issues that may have slipped through preventive measures. They provide evidence of losses but cannot prevent them from happening in the first place. Examples include assess, analyses, variance analyses, reconciliations, physical inventories, and audits. Importantly, detective controls also help assess the effectiveness of preventive controls (Wells, 2006).

2.2.5.3 Corrective Controls:

Corrective controls, as defined by (Simmons, 1995), aim to rectify any deviations or issues identified within the system. These controls can take various forms, including system redesign, follow-up procedures, post-implementation audits, and disciplinary actions for non-compliance (Simmons, 1995).

2.2.5.4 Directive Controls

Management establishes directive controls**,** such as policies and procedures, to guide employees towards adhering to independence regulations (Rittenberg, 2007). These policies and procedures should be well-disseminated throughout the organization and maintain clarity and consistency to ensure effective compliance.

2.2.5.5 Compensating Controls:

Companies may implement workarounds to address gaps in their control systems. For instance, a firm with a digital client database might keep a printed backup in the office for emergencies. This paper copy would serve as a contingency plan in case of electronic system outages or difficulties in searching the digital database.

2.2.6 Components of Internal Control Systems:

Widely adopted in finance, the COSO framework identifies five interdependent components that contribute to a well-designed internal control system.

2.2.6.1 Control Environment:

The foundation of internal controls lies within the organization's control environment ((COSO)., 2013). This environment fits the overall tone voice at the upside, emphasizing ethical conduct and integrity end-to-end all levels ((COSO)., 2013). It encompasses elements like corporate governance, management philosophy, and a strong risk awareness culture.

Arguably, the most critical aspect of the control environment is the influence it exerts on individual mindsets within the organization (Ramos, M., 2004). It shapes how employees approach their roles and their understanding of the importance of internal controls (Ramos, 2004). (Rae., 2006), concur, highlighting that an organization's workforce is its driving force, and their individual attributes significantly impact success. These attributes include not only competence but also ethical values and integrity (Rae., 2006). Ultimately, the control environment, established by management, sets the standard for these values and behaviors (Rae., 2006).

An organization's control environment is shaped by its leaders' and employees' honesty and ethics, the overall skill level of its staff, and how well its audit committee functions.(Rae., 2006).

2.2.6.2 Risk Assessment:

According to the COSO framework, the key step following establishing a strong control environment is risk assessment, which involves actively searching for and understanding potential threats to achieving an organization's goals. (COSO, 2013). This process involves identifying and analyzing potential threats, including fraud that could jeopardize the organization's goals (IIA, 2017). By assessing the likeliness and potential impact of each risk, organizations can prioritize the implementation of control activities (IIA, 2017).

Effective risk assessment is crucial for navigating today's dynamic business environment. Businesses constantly face internal and external challenges that can derail their objectives (Martin, 2010). Proactive risk assessment allows organizations to identify vulnerabilities and take steps to minimize them, ultimately promoting organizational resilience (Martin, 2010).

The COSO framework outlines key principles for conducting effective risk assessments within internal controls (COSO, 2013). These principles include:

Clearly defining organizational objectives: This clarity allows for a more targeted identification and assessment of relevant risks. Identifying and analyzing risks across the organization: A comprehensive approach ensures all potential threats are considered. Explicitly evaluating fraud risk: Fraud is a significant threat, so specifically assessing its potential impact is essential. Adapting to change: The risk landscape can evolve, so continuous monitoring and adjustments to the internal control system are necessary.

2.2.6.3 Control Activities:

Implement specific policies and procedures to mitigate identified risks and prevent fraud.

Examples include separation of duties, authorization procedure, physical and logical access controls, and reconciliations (COSO, 2013).

The organization implements safeguards at all levels and across different areas to manage risks. The organization uses a combination of manual procedures and automated systems

to act as safeguards against risks that could jeopardize its success in achieving its goals and mission. According to Jenkinson (Jenkinson, 2008), having clear rules and steps (control policies and procedures) is essential to make sure the institution achieves its goals efficiently. To manage risks, organizations implement various control activities, such as requiring approvals for actions, verifying information, and reconciling accounts, evaluating performance, protecting assets, and dividing responsibilities among staff. Another key aspect of controls is monitoring performance. This involves comparing actual results to budgets, forecasts, and past performance, with a focus on specific areas like compliance, finances, or operations. In banking, reviews often place a strong emphasis on these aspects to ensure the bank is following regulations, managing finances effectively, and operating smoothly. According to Ramos (Ramos, M., 2004), this research highlights the importance of strong controls to guarantee information and transactions are accurate, complete, and authorized. This includes carefully managing the development of new systems and updates to existing ones. Additionally, restricting access to programs and data is essential for security. Physical controls encompass managing equipment, inventories, securities, cash, and other assets, ensuring their physical security and periodically reconciling them with control records. Performance indicators can be used to anticipate expected operating outcomes and investigate unexpected results that may hinder the achievement of the bank's objectives. To minimize the risk of errors or inappropriate actions, different individuals should be assigned distinct duties. An important control measure is the segregation of duties. This means separating tasks like approving transactions, recording them in the accounting system, and having custody of the assets involved (like cash or inventory) among different employees.

2.2.6.4 Information and Communication:

Effective internal controls rely on a smooth flow of accurate information throughout the organization (IIA, 2017). This forth component, information and communication, ensures relevant details are readily available to authorize personnel for informed decision-making and to identify potential fraud.

Information systems, like accounting software, are crucial tools for gathering and analyzing data that supports effective management and control activities (Lamoye., 2005). Timely and accurate information, accessible in a suitable format, empowers employees to fulfill their internal control and operational responsibilities (Lamoye., 2005). An effective control system relies on everyone in the organization understanding their role within it. This includes knowing how their tasks connect to the work of others and their individual responsibility for upholding the system. Clear information sharing and communication channels are essential for achieving this awareness. Communication extends beyond internal boundaries. External parties like customers, suppliers, and regulators also require relevant information for effective interactions ((COSO)., 2013). The updated COSO framework outlines key principles for a robust information and communication system:

2.2.6.5 Monitoring Activities:

The control system should be constantly evaluated to see if it's working properly. This helps identify areas where it can be strengthened to better manage risks. This involves internal audits, independent reviews, and ongoing monitoring of control activities (COSO, 2013). Whittington & Pany (Pany, O. Ray Whittington & Kurt, 2001) explain that an organization monitors its operations and transactions by carefully observing them. This ongoing process helps assess how well things are going (performance quality) over time, and importantly, how effective the implemented controls are at managing risks. To ensure optimal results, management should direct their monitoring efforts towards internal control and the successful accomplishment of organizational goals. A crucial aspect of effective monitoring is ensuring it is essential for all employees to have a thorough grasp of organization's mission, objectives, responsibilities, as well as the levels of risk tolerance.

As per (Muhota, 2005), monitoring holds significant importance within the internal control framework of banking institutions. While regulatory and supervisory measures are adopted by central banks externally, monitoring serves as an internal tool. It involves

a continuous process of periodically conducting procedures as well as analyzing internal records from banks. This ensures completion of all mandatory protocols carried out in accordance with the set standards.

2.2.7 Fraud Theory:

Understanding the drivers and types of fraud is essential for designing effective ICS. The Fraud Triangle, proposed by (Cressey D. , 1973), identifies three key factors that contribute to fraud: pressure, opportunity, and rationalization. Pressure arises from financial difficulties or personal challenges, opportunity refers to vulnerabilities in control systems that allow fraudulent acts to occur, and rationalization involves justifying the wrongdoing to oneself. Additionally, (Wolfe, D. T., & Beaumaris, A. L., 2007) proposed the Occupational Fraud Triangle, expanding upon Cressey's model to include organizational factors such as poor leadership, weak ethical culture, and inadequate oversight.

2.2.8 Classification of Fraud:

Understanding different types of fraud is crucial for designing effective ICS. Common classifications include:

Asset Misappropriation: Theft or misuse of organizational assets for personal gain, such as embezzlement or cash larceny ((ACFE)., 2008). Corruption: Bribery, extortion, or kickbacks involving employees and external parties (World Bank. , 2017). Financial Statement Fraud: Intentional misrepresentation of financial records to deceive stakeholders ((AICPA)., 2016).

2.2.9 Causes of Bank Frauds:

Several factors contribute to the vulnerability of banks to fraud, including:

Increased complexity of financial products and services: Makes it harder to detect fraudulent activities within intricate transactions. Pressure to meet performance targets: Can incentivize employees to engage in risky or unethical behavior. Weak internal controls: Inadequate control systems create opportunities for fraud to occur. Technological advancements: New technologies can present new avenues for fraudsters to exploit. Collusion between employees and external parties: Increases the difficulty of detection and prosecution (PwC., 2019).

2.2.10 Anti-Fraud Controls:

Effective ICS should implement various anti-fraud controls to mitigate risks and deter fraudulent activities. Examples include:

A critical defense against fraud is a strong system of internal controls (ICs). These controls work together to prevent, detect, and deter fraudulent activity. One key principle is segregation of duties, which separates critical financial functions like authorization, recording, and custody. This prevents a single person from controlling the entire process, making it more difficult to manipulate records or steal assets. Authorization procedures add another layer of security by requiring proper approvals for significant transactions. This ensures only authorized personnel can initiate high-risk activities, reducing the chance of unauthorized access or misuse of funds.

Physical and logical access controls further safeguard sensitive information and systems. By restricting access based on roles and responsibilities, only authorized individuals can view or modify critical data. This can involve physical security measures like locked doors or keycard access, as well as logical controls like passwords and user permissions within computer systems. Regular reconciliations are another important tool. Comparing accounts and records helps identify discrepancies that might indicate fraudulent activity.

Inconsistencies between financial statements, inventory counts, or bank statements can be red flags that warrant further investigation. Independent reviews, both internal and external audits, provide a critical outside perspective. These assessments not only evaluate how effective internal controls are, but also identify potential weaknesses that fraudsters could exploit. Regular audits are essential for guaranteeing the reliability of financial statements. They also help to deter potential misconduct.

Finally, education is crucial. Fraud awareness training equips employees to recognize fraud risks and empowers them to report suspicious activities. By understanding the common tactics used by fraudsters, employees can be a valuable first line of defense (Association of Certified Fraud Examiners (ACFE)., 2018). Several researchers have identified a model known as the fraud triangle, which highlights three key factors that contribute to fraudulent activity: pressure/incentives, opportunity, and rationalization (Cressey D. R., 1953). When an individual has a motive (like financial pressure), an opportunity (like weak controls), and a way to justify it (rationalization), the risk of fraud becomes significant. (Cressey D. R., 1953). Among these factors, opportunity is considered the most manageable (Cressey D. R., 1953). Effective control environments can be designed to limit opportunity and deter fraudulent behavior across all levels of the organization, including employees, vendors, consultants, and senior management (Cressey D. R., 1953). One approach to building such an environment involves implementing five key anti-fraud controls, with "tone at the top" being the first and most crucial element (Cressey D. R., 1953).

1 Prevent: A Truly Empowering Independent and Empowered Audit Committee

Effective anti-fraud programs rely heavily on a strong and independent audit committee ((COSO)., 2013). Organizations with stakeholders independent of management benefit from an audit committee that functions without undue influence ((COSO)., 2013). This independence fosters a healthy dose of skepticism, encouraging the committee to continuously evaluate the organization's anti-fraud controls and programs ((COSO)., 2013).

The audit committee plays a critical function in supervise internal controls and fraud risk management. Key responsibilities include monitoring the results of internal audits and quarterly reviews, as well as providing direction for the internal audit department ((COSO)., 2013). Research suggests that internal and independent auditors combined detect roughly 29% of occupational fraud ((ACFE)., 2008). While independent auditors follow established standards (SAS 99) to identify potential fraud in financial statements, empowered audit committees can play a more proactive role ((ACFE)., 2008). By providing direction and monitoring internal audit activities, these committees can ensure that audit procedures target areas with the highest fraud risk ((ACFE)., 2008). Effectively identifying such areas often requires a thorough fraud risk assessment ((ACFE)., 2008).

2 Prevent: Conduct Detailed Fraud Risk Assessments

The Public Company Accounting Oversight Board (PCAOB) Standard No. 5 (2007) emphasizes the importance of annual risk assessments for public companies (PCAOB, 2007). These assessments help identify key controls in areas with significant risk, including fraud (PCAOB, 2007). A well-designed fraud risk assessment serves several purposes. First, it focuses management's attention on the most critical fraud risks facing the organization (Examiners & (ACFE)., 2018).

Effective fraud risk assessments are typically recurring and systematic, involving various levels of management across different business functions (Examiners & (ACFE)., 2018). The assessment process may consider specific fraud schemes that could potentially target the organization (Examiners & (ACFE)., 2018). This includes identifying potential perpetrators within the organization, the likelihood of each scheme occurring, and the potential financial impact (Examiners & (ACFE)., 2018). By analyzing the identified fraud schemes, we can assess how well-suited our existing internal controls are to prevent or detect them and to determine their effectiveness in mitigating these risks (Examiners & (ACFE)., 2018). For significant fraud risks not addressed by current controls, a gap analysis with a remediation plan can be included (Examiners & (ACFE)., 2018).

While some organizations possess the internal resources for conducting effective fraud risk assessments, many can benefit from using an external provider (Examiners & (ACFE)., 2018). External providers can facilitate brainstorming sessions and interviews to ensure these activities are focused and relevant (Examiners & (ACFE)., 2018). This approach can also enhance the visibility of management's commitment to fraud risk management throughout the organization (Examiners & (ACFE)., 2018). Increased communication about fraud by management can lead to greater employee awareness of the importance of ethical behavior and the confidence to report suspicious activities (Examiners & (ACFE)., 2018).

3 Deter & Detect: Building a Culture of Reporting: Tools for Identifying and Preventing Wrongdoing

In order to protect against fraud and wrongdoings, the Sarbanes-Oxley Act requires company audit committees to set up a system for employees to confidentially report any concerns they have. This system should allow employees to submit complaints and ensure they are properly investigated. (Sarbanes-Oxley Act of 2002,, 2002). Whistleblower hotlines offer a convenient and cost-effective way to fulfill this requirement (Sarbanes-Oxley Act of 2002,, 2002). Research suggests that whistleblower tips contribute to the detection of approximately 46% of all occupational fraud cases (Examiners & (ACFE)., 2018).

Simply having a whistleblower hotline is not enough. Organizations should conduct periodic evaluations to assess the hotline's effectiveness (Examiners & (ACFE)., 2018). This evaluation may include benchmarking the hotline against industry best practices (Examiners & (ACFE)., 2018). To further enhance the perception of confidentiality, companies can consider using an experienced external provider to manage the hotline (Examiners & (ACFE)., 2018). Alternatively, if an internal body manages the hotline, complaints should be reviewed initially by an ethics committee with direct access to the audit committee (Examiners & (ACFE)., 2018). Furthermore, to capture potential bribery and corruption, companies should extend whistleblower hotline access to vendors and customers in addition to employees (Examiners & (ACFE)., 2018).

For organizations operating globally, offering a 24/7 multilingual hotline is recommended (Examiners & (ACFE)., 2018). Most importantly, consistent communication regarding the hotline's availability is crucial (Examiners & (ACFE)., 2018). At least annually, companies should communicate the hotline's existence and encourage employees to report suspicious activity by providing examples of reportable behaviors (Examiners & (ACFE)., 2018).

4 Prevent & Deter: Building a Strong Defense: Anti-Fraud Policies and Empowering Training

Confusion regarding what constitutes fraud or misconduct can lead to employee behavior that erodes an organization's resources (Examiners & (ACFE)., 2018). For example, some employees might exploit expense reimbursement policies by neglecting to submit receipts for smaller amounts (Examiners & (ACFE)., 2018). Similarly, engaging in side businesses during work hours using company resources represents another form of misuse (Examiners & (ACFE)., 2018). While these activities may seem insignificant, they contribute to a culture that tolerates unethical behavior (Examiners & (ACFE)., 2018). Furthermore, research suggests that fraudulent schemes often begin small and escalate over time as perpetrators gain confidence (Examiners & (ACFE)., 2018).

A well-defined anti-fraud policy can address this confusion by explicitly outlining prohibited behaviors ((AFE)., 2016). This policy should include clear definitions of fraud and misconduct, along with specific examples relevant to the organization's context ((AFE)., 2016). By clearly communicating expectations, the policy discourages misunderstandings about acceptable conduct ((AFE)., 2016).

Publishing the anti-fraud policy is just the first step. The organization offers regular training sessions at all levels to foster discussions about the importance of ethical conduct in the workplace (Examiners & (ACFE)., 2018). These training programs can delve deeper into the definitions outlined in the policy and provide practical guidance for identifying and reporting suspicious activity (Examiners & (ACFE)., 2018). The policy can further detail the organization's approach to handling reports of wrongdoing,

underscoring its commitment to open communication and taking responsibility for addressing such issues (Examiners & (ACFE)., 2018).

5 Deter & Detect: Upholding Integrity: Effective Procedures for Investigating Fraud Allegations

No matter the nature or severity of a fraud allegation, organizations should have a documented policy outlining the investigation and resolution process (Examiners & (ACFE)., 2018). This policy typically establishes procedures for preserving documentation and gathering evidence (Examiners & (ACFE)., 2018). The policy should clearly outline who within the organization will be responsible for taking action (responsible), ultimately answer for the outcome (accountable), provide necessary input (consulted), and be kept up-to-date (informed) depending on the specific nature of the allegation. This ensures a clear and coordinated response to any reports of misconduct (Examiners & (ACFE)., 2018).

Similar to conducting fraud risk assessments, some organizations may have qualified personnel on staff, as well as specialists such as certified fraud examiners (CFEs), attorneys, and certified public accountants (CPAs), who can conduct internal investigations (Examiners & (ACFE)., 2018). However, for allegations involving potentially material financial statement impacts or senior management, leading practices recommend using independent attorneys or other third-party specialists (Examiners & (ACFE)., 2018). Having a documented policy and adhering to it can be particularly beneficial if relevant regulatory bodies, like the SEC or DOJ, launch an investigation (DOJ) takes an interest in the allegation (Examiners & (ACFE)., 2018).

Unfortunately, fraud can occur in any organization (Examiners & (ACFE)., 2018). Internal controls are susceptible to becoming outdated as technology evolves or due to deliberate actions by individuals. This can include situations where management bypasses established procedures or employees conspire to circumvent controls (Examiners & (ACFE)., 2018). Implementing these five anti-fraud controls is a crucial step, but it doesn't completely eliminate the risk of fraud, they significantly strengthen an

organization's control environment (Examiners & (ACFE)., 2018). Effective anti-fraud programs communicate a clear message of senior management's commitment to preventing and detecting fraud, deterring potential perpetrators (Examiners & (ACFE)., 2018).

2.3 Empirical Review:

2.3.1 International Researches

A research by (Leah N., & Dr. Josiah A., 2017), investigated the link between internal controls and fraud in Kenyan commercial banks. Employing an explanatory research design to establish cause-and-effect relationships, their research examined all 43 Kenyan commercial banks during the specified period. A census survey was conducted with thirteen banks, and the five internal control components were considered as the dependent variables, while fraud prevention and detection were treated as the independent variable. Using primary data analyzed through an ordinary linear regression model with SPSS version 20, it's important to note that the research found a negative correlation, meaning that having more internal controls wasn't necessarily linked to better fraud prevention/detection. This suggests that stronger controls might be associated with lower fraud detection rates, which contradicts some existing research and highlights a need for further investigation (Leah N., & Dr. Josiah A., 2017).

In a research titled "Evaluating the Effectiveness of the Control Environment and Monitoring Activities Components of Internal Control Systems of Ghanaian Banks" (Ayagre, W., Darkwah, N. A., & Adusei, M., 2014), researchers assessed these aspects using the COSO framework. They employed a survey with a five-point Likert scale to gauge respondents' understanding and perception of internal controls, along with the overall effectiveness of the banks' systems. Statistical analysis of the data was performed using the software SPSS. The findings, presented as average scores and standard deviations for each survey section, indicated strong controls within both the control environment (average mean: 4.72) and monitoring activities (average mean: 4.66) (Ayagre, W., Darkwah, N. A., & Adusei, M., 2014).

In their research, (Anjali, V. E., Amuda, O. O., & Arulogun, O. A., 2013), assessed the effectiveness of internal control systems in preventing fraud within the Nigerian banking industry. The research employed archival data, analyzing the published financial statements of five commercially audited Nigerian banks. To assess the relationship between ICS and fraud, the authors utilized product-moment correlation coefficients and regression analysis. Their findings indicated a significant positive association, suggesting that a robust internal control system can help prevent and curb fraud within Nigerian banks. The research further concluded that poor corporate governance practices might hinder the proper design and implementation of ICS, potentially impacting the overall performance of Nigerian banks.

(Joseph, A., Albert, L., & Byaruhanga, E., 2012), examined the influence of internal controls on fraud detection and prevention within district treasuries of Kakamega County, Kenya. To gather information, the researchers used a mix of techniques. This included analyzing data to describe trends (descriptive) and drawing conclusions based on those trends (inferential statistics). Data was collected through surveys and analyzed using SPSS software. The research found a strong connection between having well-designed control systems and treasuries being able to successfully prevent and identify fraud. (Joseph, A., Albert, L., & Byaruhanga, E., 2012). This suggests that stronger internal controls can significantly contribute to hindering and uncovering fraudulent activity. Based on these findings, the authors recommend implementing cost-effective and effective control policies and procedures to mitigate fraud risks in these institutions (Joseph, A., Albert, L., & Byaruhanga, E., 2012).

(Atuk, 2011), research, "The Effectiveness of Internal Control Systems in Nigerian Banks," examined the internal controls within five Nigerian banks (Diamond Bank Plc., Eco bank Nigeria Plc., First Bank of Nigeria Plc., United Bank for Africa Plc., and Zenith International Bank). This mixed-methods research employed a combination of questionnaires, observations, and interviews conducted across various departments within each bank. Notably, these banks were selected from a larger pool of 24 institutions

operating in Nigeria. Following a comprehensive analysis of the data, the research supported the importance of internal controls in Nigerian banks. Atuk's assessment is that these controls provide a strong level of confidence that the bank runs smoothly and efficiently, produces trustworthy financial statements, and follows all applicable laws and regulations.

2.3.2 Local Researches

(Tekalegn, 2019), research looked at how well internal controls work at a branch of the Commercial Bank of Ethiopia in Hawassa. The researcher used a survey with a mix of multiple choice and open-ended questions that employees filled out themselves. The research revealed the bank's internal controls to be effective in several areas, including the presence of clear codes of conduct, periodic management review of policies and procedures, well-communicated organizational objectives for risk assessment, adequate separation of duties with dual controls, and effective reporting procedures communicated to employees.

(Fikru Worku., 2018), research focused on Ethiopian banks to see how weaknesses in internal controls are linked to fraud. It examined the current situation (descriptive design) to understand how often fraud happens when controls are lacking. The author utilized a survey method, distributing questionnaires to internal audit staff and management personnel across various Ethiopian banks. The collected data focused on the prevalence of different internal control weaknesses and their association with reported fraud incidents. (Fikru Worku., 2018), findings revealed that the more weaknesses there were in a bank's internal controls, the more likely it was that fraud would occur in Ethiopian banks. This suggests that strengthening internal controls within Ethiopian banks could be a crucial step in mitigating fraud risks.

(Ashenafi, 2017), investigated the internal control system within a microfinance institution (MFI), emphasizing their critical role in national development through financial services for low-income populations. Prior research highlighted internal control weaknesses as a key MFI challenge. This research assessed the MFI's system using a

survey method (questionnaires for employees and semi-structured interviews with management) to identify potential deficiencies. Data analysis with SPSS software (frequency tables, means, and standard deviations) revealed a satisfactory overall internal control system. The research found that all five control components were in place, with risk assessment being the strongest (averaging a score of 3.81 out of 5). This indicates a strong focus on identifying potential risks.

(Alemayehu, 2016), investigated how well the Development Bank of Ethiopia manages its internal controls. They used a survey with employees (quantitative approach) to analyze five key areas: the overall control environment, the specific controls in place, how well risks are assessed, how information is shared, and how controls are monitored over time (control environment, control activities, risk assessment, information and communication, and monitoring). The research design aimed to explain the relationships between these areas and the effectiveness of the internal control system (explanatory design). Descriptive analysis revealed concerning results, with mean scores for all components falling below three (presumably on a five-point scale). This aligned with over 80% of respondents disagreeing with the bank's control effectiveness in each area. (Alemayehu, 2016), suggests policy changes to address these weaknesses, including proper duty segregation, enhanced computer security, and stricter review processes for credit, purchases, and procedures. Additionally, the bank should implement periodic risk assessments to identify risk tolerance, high-risk areas, and mitigation strategies.

2.4 Conceptual Framework

This research plan described the important connections between a well-designed system of internal controls (ICS) and how well it helps Global Bank Ethiopia S.C. prevent and identify fraud. It drew upon established theories, frameworks, and empirical evidence from both global and Ethiopian contexts to provide a roadmap for analyzing the bank's control mechanisms and their contribution to mitigating fraud.

2.4.1 Independent Variables:

Effectiveness of Global Bank Ethiopia's S.C ICS: This encompassed the overall strength and efficiency of the bank's ICS in preventing and detecting fraudulent activities. It was assessed through various measures like the adequacy of control activities, the quality of risk assessment procedures, and the effectiveness of monitoring mechanisms.

2.4.2 Dependent Variables:

Fraud Prevention: This measured the extent to which Global Bank Ethiopia's S.C ICS deterred fraudulent activities from occurring. Indicators included the number and types of fraud attempts prevented, financial losses avoided due to effective controls, and the overall reduction in fraud risk exposure.

Fraud Detection: This measured the ability of the ICS to identify and uncover fraudulent activities that may have already taken place. It was assessed by analyzing the timeliness and accuracy of fraud detection, the effectiveness of investigative procedures, and the success rate of recovering misappropriated funds or assets.

2.4.3 Conceptual Model:

The following diagram visually represented the relationships between variables within the conceptual framework:

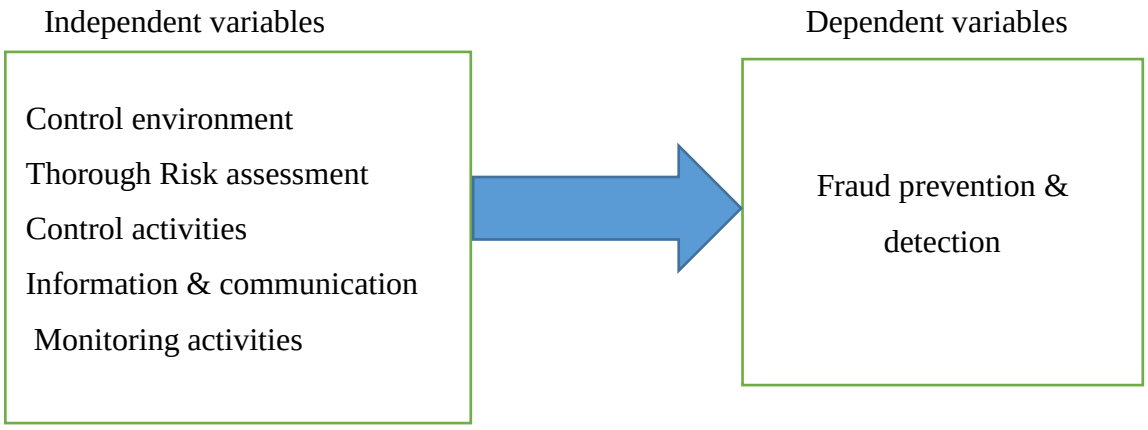

Figure 1 : Conceptual Framework model

Source: ((COSO)., 2013)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the methodological framework employed to investigate the relationship between the effectiveness of Internal Control Systems (ICS) and their role in preventing and detecting fraud within Global Bank Ethiopia S.C (GBE). An explanatory research design was utilized to test hypotheses that explain how internal control effectiveness influences fraud prevention and detection rates. To collect new information directly from employees (primary data), the researcher used a survey. The researcher chose a specific method (stratified random sampling) to make sure the survey included employees from different departments at Global Bank Ethiopia (GBE), giving a more accurate picture of the whole bank.

3.2 Research Design and Approach

The research methodology serves as the roadmap for a research, guiding researchers through the process of formulating research questions and objectives, collecting data, and ultimately presenting the findings (Denzin, 2017). This framework ensures a logical and systematic approach to inquiry, allowing researchers to draw well-supported conclusions from the information gathered during the investigation.

To investigate the factors influencing the effectiveness of Global Bank Ethiopia's S.C (GBE) internal control system (ICS) in preventing and detecting fraud, this research adopted an explanatory design with a quantitative approach. This methodology is well-suited for uncovering cause-and-effect relationships between variables (Sekaran, 2003). A structured questionnaire served as the primary data collection tool, focusing on questions that assess the effectiveness of GBE's ICS components. This design choice allowed the research to identify patterns and causal links between these components (independent variables) and the prevalence of fraud (dependent variable). By employing a quantitative approach, the research aimed to provide a comprehensive explanation for "why" the ICS is effective in deterring and uncovering fraudulent activity.

In order to meet the research's aims, an explanatory research design was used in order to allow the researcher to make to an appropriate level of conclusion. This research adopted an explanatory design with a quantitative approach to investigate the factors influencing the effectiveness of Global Bank Ethiopia's S.C (GBE) internal control system (ICS) in preventing and detecting fraud (Sekaran, 2003). Explanatory research is particularly well-suited for this research because it aims to uncover cause-and-effect relationships between variables, rather than simply describing a phenomenon or identifying correlations (Sekaran, 2003).

3.3 Data type and collection method

To gather quantitative data from a large sample of participants, the research employed a structured questionnaire as the primary data collection tool (De Vaus, 2002). This standardized approach ensured consistency in data collection and facilitated efficient administration (De Vaus, 2002). The researcher carefully crafted a survey to answer the research questions. The survey included multiple choice questions (closed-ended) to gather specific details (factual information) about different aspects of the internal control system (ICS) and fraud, while Likert scale questions captured participants' attitudes and opinions on these same variables.

3.4 Population and Sampling Technique

To ensure the questionnaire's effectiveness, a pilot test was conducted with a small group representative of the target population (employees of Global Bank Ethiopia S.C) (De Vaus, 2002). This pilot phase assessed question clarity, response options, and overall flow, allowing for refinements before administering the final questionnaire to the main sample (De Vaus, 2002).

Given the potentially large size of GBE's employee base, to get a good cross-section of employees, the researcher used a method called purposive and convenient sampling (Rea, L. M., & Parker, R. A. , 2014). In order to get a representative sample, researcher use a technique called purposive. This involves breaking down the entire group (population) into smaller subgroups based on features that are important to the question they are trying

to answer. In this case, the purposive and convenient method included employees directly involved in internal controls, fraud risk management, or relevant departments. By using purposive and convenient, the researcher made sure the people who answered the survey (participants) had the relevant knowledge and experience to give reliable information (valuable insights) on how well the internal control system (ICS) works to prevent and catch fraud. (Rea, L. M., & Parker, R. A. , 2014).

While random sampling is often considered ideal, it might have presented logistical challenges within GBE. Purposive sampling offered a practical alternative by focusing on a representative subsample with the most relevant information for the research (Rea, L. M., & Parker, R. A. , 2014).

The final sample size of 57 participants was determined through a purposive and convenience method. This statistical technique considers factors like anticipated effect size (the strength of the relationship between variables), desired confidence level (the probability that the sample reflects the population), and acceptable margin of error (the allowable deviation between sample and population values) (Kothari, 2004). Following the principles outlined in (Kothari, 2004), the power analysis ensured the sample size was sufficient to yield statistically reliable results (Kothari, 2004).

3.5 Analysis and Evaluation of Data

The researcher used a computer program called SPSS to analyze the information that the researcher collected from the survey. First, the researcher used descriptive statistics to get a basic understanding of the data, like finding averages and frequencies. This involved techniques like frequencies (counts of occurrences for categorical variables), means (averages for continuous variables), and standard deviations (measures of spread for continuous variables). These initial analyses provided a foundational understanding of the data's central tendencies and variability.

Once the researcher had a summary of the data (descriptive analysis), the researcher used more advanced statistics (inferential statistics) to test researcher’s idea about how different factors might be linked (hypotheses about relationships between variables). This

allowed the researcher to draw conclusions that apply not just to the specific group they studied (sample) but to the wider population they represent.

3.6 Validity

This research prioritized both internal and constructs validity. Internal validity ensured the findings reflected true cause-and-effect relationships, not extraneous factors. Utilizing a structured questionnaire and employing reliable statistical methods contributed to internal validity. Construct validity focused on whether the measures used accurately captured the intended concepts. Careful questionnaire development, pilot testing, and ensuring question clarity enhanced construct validity.

3.7 Reliability

Reliability referred to the consistency and reliability of the research findings. This research promoted reliability by employing a standardized questionnaire and clear data collection procedures. Additionally, utilizing reliable statistical methods and reporting detailed methodology increased the likelihood of replicating the research and obtaining similar results.

3.8 Expected Results and Output of the Study

The research outcome identified and analyzed the key factors influencing the effectiveness of ICS in preventing and detecting fraud within the GBE. The analysis revealed statistically significant relationships between variables, leading to a comprehensive understanding of the "why" behind the effectiveness of ICS. The research output included a detailed report outlining the research methodology, findings, conclusions, and potential implications for practice within the GBE.

3.9 Conclusion

This chapter described the step-by-step plan (methodological framework) the researcher used for his quantitative research. The research aimed to find out how effective the internal control system (ICS) is at preventing and detecting fraud at Global Bank Ethiopia (GBE). Quantitative research methods focus on collecting numerical data. The explanatory research design, stratified sampling technique, and structured questionnaire offered a robust approach to gathering and analyzing data on the topic. The emphasis on validity and reliability ensured the credibility of the findings. This research provided valuable insights into the effectiveness of ICS and potentially contributed to positive changes within the GBE.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION, INTERPRETATION AND DISCUSSION

4.1 Introduction

This chapter analyzes survey findings to explore the connection between a strong internal control system (ICS) and fraud prevention and detection at Global Bank Ethiopia S.C. The author examines the effectiveness of their ICS using descriptive statistics to understand its role in fraud control. Then, to assess the relationship between ICS and fraud, the author present diagnostic test results and regression analysis findings. Finally, the author discusses the implications and summarizes the key takeaways from the data analysis of the employee survey responses.

4.2 Respondents Profile

4.2.1. Sex And Age Distribution

Table 1: Descriptive Statistics of Sex of Respondents

Sex of the respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	34	59.6	59.6	59.6
	Female	23	40.4	40.4	100.0
	Total	57	100.0	100.0	

Source: questionnaire and SPSS output (2024)

The survey participants were mostly male (59.6%) with females making up the remaining 40.4%. In other words, for every 100 respondents, there are about 60 males and 40 females.

Table 2: Descriptive Statistics of Age of Respondents

Age of the respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20-25	18	31.6	31.6	31.6
	28-35	18	31.6	31.6	63.2
	36-42	19	33.3	33.3	96.5
	43-50	1	1.8	1.8	98.2
	Above 50	1	1.8	1.8	100.0
	Total	57	100.0	100.0	

Source: questionnaire and SPSS output (2024)

Considering the age groups of the survey participants (as illustrated above), the largest age group is 36-42yrs old, with 19 respondents (33.3%). The second largest groups are 20-25yrs and 28-35yrs old, with 31.6 respondents (31.6%). Among the respondents 1.8% falls within 43-50yrs and the remaining 1.8% were above 50yrs. Most of the respondents (around 63.2%) are younger than 36 years old.

4.2.2. Education and Work Experience

Table 3: Descriptive Statistics of Education Level of Respondents

Education level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Diploma	1	1.8	1.8	1.8
	B.A	34	59.6	59.6	61.4
	M.A/MSc	22	38.6	38.6	100.0
	Total	57	100.0	100.0	

Source: questionnaire and SPSS output (2024)

The data shows that a majority of the respondents (59.6%) have a B.A. degree, while 38.6% have M.A. /MSc degree and the remaining 1.8% has Diploma.

Table 4: Descriptive Statistics of Work Experience of Respondents

How long have you been working at Global Bank Ethiopia?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-5	32	56.1	56.1	56.1
	6-10	16	28.1	28.1	84.2
	11-15	8	14.0	14.0	98.2
	16-20	1	1.8	1.8	100.0
	Total	57	100.0	100.0	

Source: questionnaire and SPSS output (2024)

A majority of employees (56.1%) have been with Global Bank Ethiopia S.C for 1-5 years. The next largest group (28.1%) has been there for 6-10 years. Relatively fewer employees have been with the bank for longer tenures (11-15 years, 16-20 years) 8 and 1 respondents respectively. This table suggests that Global Bank Ethiopia S.C has a relatively young workforce, with a majority of employees having less than 10 years of experience at the bank.

Table 5: Descriptive statistics of location of respondents

Which location do you work at?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Branch	26	45.6	45.6	45.6
	Head office	31	54.4	54.4	100.0
	Total	57	100.0	100.0	

Source: questionnaire and SPSS output (2024)

The data on respondent locations suggests that nearly half of the respondents work at head office locations (54.4%), while the other half work at branches (45.6%).

Table 6: Descriptive Statistics of Job Title of Respondents

What is your job title/position?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Accountant	5	8.8	8.8	8.8
	Branch Manager	6	10.5	10.5	19.3
	Cashier	1	1.8	1.8	21.1
	Credit follow up and monitoring officer	1	1.8	1.8	22.8
	Customer service officer	8	14.0	14.0	36.8
	Junior Customer service Officer	2	3.5	3.5	40.4
	Manager	2	3.5	3.5	43.9
	Manager IT	1	1.8	1.8	45.6
	Manager, customer relationship management	1	1.8	1.8	47.4
	Messenger	1	1.8	1.8	49.1
	Principal Auditor	7	12.3	12.3	61.4
	Principal Innovation and Research Officer	1	1.8	1.8	63.2
	Principal kyc officer	1	1.8	1.8	64.9
	Principal Officer	3	5.3	5.3	70.2
	Principal Risk Officer	1	1.8	1.8	71.9
	Senior Customer service officer	1	1.8	1.8	73.7
	Senior Loan Officer	1	1.8	1.8	75.4
	Senior officer	2	3.5	3.5	78.9
	Senior Officer	8	14.0	14.0	93.0
	Senior Risk Officer	2	3.5	3.5	96.5
	Trade Service Officer	1	1.8	1.8	98.2
	Trainee banker	1	1.8	1.8	100.0
	Total	57	100.0	100.0	

Source: questionnaire and SPSS output (2024)

The employee survey reveals a diverse workforce at the company. Customer service roles (customer service officer, junior customer service officer, senior customer service officer)

make up a significant portion (22.8%) of the employees. Principal auditors (12.3%) form the next largest group. Branch managers (10.5%) and accountants (8.8%) hold important positions as well. There's a range of specialized roles present too, including credit follow-up officer, IT manager, and trade service officer, although each represents a smaller percentage of the total workforce. Interestingly, the title "Senior Officer" appears twice, potentially indicating different seniority levels within specific departments.

4.3 Measuring effectiveness of components of internal control system

4.3.1 A strong Control Environment

Table 7: Descriptive Statistics of Effectiveness of Control Environment

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
The bank promotes a strong ethical culture that emphasizes honesty and integrity.	57	1	5	3.47	1.283
Management demonstrates a clear commitment to preventing and detecting fraud.	57	1	5	3.49	1.212
There are formal written policies and procedures for internal control activities.	57	1	5	4.02	.973
Employees are adequately trained on fraud risks and control procedures.	57	1	5	3.44	1.053
Effective Control Environment	57	1	5	3.55	.921
Valid N (list wise)	57				

Source: questionnaire and SPSS output (2024)

The mean scores for all four statements range from 3.44 to 4.02, falling around the middle of the rating scale (assumed to be 1-5). This indicates that employees generally agree that the bank promotes an ethical culture, management is committed to fraud prevention, there are formal control procedures, and employees receive adequate training.

The standard deviation for all statements is less than 1.5, suggesting a relatively narrow range of responses. This means that there's not a large variation in opinions among employees regarding the control environment. The minimum score of 1 for all statements indicates that some employees believe there's room for improvement in the control environment. Conversely, the maximum score of 5 suggests that some employees perceive a strong control environment.

The statement that received the highest average rating (4.02), was about the existence of formal written policies and procedures. This suggests strength in the bank's documented controls. The statement with the lowest mean score (3.44) is about employees are adequately trained on fraud risks and control procedures. While the score is still positive, it might be worth investigating if there are areas to enhance the bank's ethical culture.

4.3.2 Risk Assessment

Table 8: Descriptive Statistics of Effectiveness of Risk Assessment

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
The bank regularly identifies and assesses the potential fraud risks it faces.	57	1	5	3.53	1.087
The risk assessment process is comprehensive and considers all relevant factors.	57	1	5	3.32	1.105
The identified fraud risks are prioritized based on their severity and likelihood.	57	1	5	3.51	1.071
Appropriate controls are implemented to mitigate the identified fraud risks.	57	1	5	3.47	1.087
Effective Risk Assessment	57	1	5	2.97	1.084
Valid N (list wise)	57				

Source: questionnaire and SPSS output (2024)

Risk assessments are a crucial component of Global Bank Ethiopia's S.C internal control system. The bank identifies and assesses potential fraud risks it faces (mean score 3.53).

However, there's room for improvement, as some employees believe the comprehensiveness of the process could be better (mean score 3.32 for considering all relevant factors). The mean scores for all four statements range from 3.32 to 3.53, falling around the middle of the rating scale (assumed to be 1-5). This indicates a general agreement that the bank regularly identifies and assesses risks, prioritizes them, and implements controls to mitigate them.

The standard deviation for all statements is less than 1.5, suggesting a relatively narrow range of responses. This means there's not a large variation in opinions among employees regarding the risk assessment process. The minimum score of 1 for all statements indicates that some employees believe there's room for improvement in risk assessment. Conversely, the maximum score of 5 suggests that some employees perceive a strong risk assessment process. The lowest mean score (3.32) is for the comprehensiveness of the risk assessment process, suggesting that some employees believe not all relevant factors are considered.

4.3.3 Control Activity

Table 9: Descriptive Statistics of Effectiveness of Control Activity

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
The bank has implemented effective controls over key financial processes.	57	1	5	3.58	1.051
Controls are designed to prevent unauthorized access to assets and records.	57	1	5	3.61	1.176
There is adequate segregation of duties to prevent fraud and errors	57	1	5	3.60	1.050
Transactions are regularly monitored and reconciled to identify discrepancies.	56	1	5	3.46	1.159
Effective Control Activity	57	1	5	3.39	1.010
Valid N (list wise)	56				

Source: questionnaire and SPSS output (2024)

The data suggests that control activities are generally perceived as positive, but there's room for improvement in some areas. Mean scores around 3.46-3.61 indicate a moderate level of agreement that the bank has implemented controls over key financial processes, designed controls to prevent unauthorized access, and segregated duties to prevent fraud. The high standard deviation (around 1.2) for some statements suggests a variation in employee perceptions. Some employees might believe the controls are very effective, while others might have reservations. The lowest mean score (3.46) for transaction monitoring highlights a potential area for improvement. It's crucial to ensure these procedures are effective in catching discrepancies.

Overall, the findings suggest that Global Bank Ethiopia S.C has a foundation for control activities, but there's an opportunity to strengthen them further. By investigating areas like transaction monitoring and segregation of duties, the bank can enhance its ICS's ability to prevent and detect fraud.

4.3.4 Information and Communication

Table 10: Descriptive Statistics of Effectiveness of Information and Communication channels

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Relevant information about fraud risks and control procedures is effectively communicated to all employees	57	1	5	3.14	1.288
There are open channels for employees to report suspected fraud without fear of retaliation	57	1	5	3.12	1.196
Management regularly reviews and updates internal control documentation.	55	1	5	3.18	1.234
Effective Information and Communication	57	1	5	3.19	.997
Valid N (list wise)	55				

Source: questionnaire and SPSS output (2024)

Mean scores ranging from 3.12 to 3.18 indicate somewhat low level of agreement that information about fraud risks and control procedures is effectively communicated or that there are open channels for employees to report suspected fraud. The standard deviation (around 1.2) suggests some variation in employee perceptions. Some employees might feel informed and comfortable reporting fraud, while others might not.

Overall, these findings suggest that communication and information sharing related to fraud prevention might be a weak spot in the ICS. Employees might not feel fully equipped to identify and report fraud.

4.3.5 Monitoring Activity

Table 11: Descriptive Statistics of Effectiveness of Monitoring Activity

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
The bank actively monitors the effectiveness of its internal control system.	57	1	5	3.26	1.126
Internal audits are conducted regularly and address all relevant control areas.	56	1	5	3.36	1.086
Management takes timely action to address any identified weaknesses in the internal control system.	57	1	5	3.63	1.159
Effective Monitoring Activity	57	1	5	3.46	.975
Valid N (list wise)	56				

Source: questionnaire and SPSS output (2024)

The bank appears to be moderately active in monitoring its ICS, but there's room for improvement in some areas. Mean scores around 3.26 indicate a somewhat low level of agreement that the bank actively monitors the system's effectiveness and conducts regular internal audits covering all relevant control areas. The standard deviation (around 1.2) suggests some variation in employee perceptions. Some might believe monitoring is thorough, while others might have doubts.

The slightly lower mean score (3.26) for internal audits covering all control areas warrants further investigation. The highest mean score (3.63) for management taking timely action on identified weaknesses is a positive sign, indicating a willingness to address control deficiencies.

Overall, these findings suggest that while Global Bank Ethiopia S.C has some monitoring activities in place, they might not be as comprehensive or frequent as they could be.

4.3.6 Effectiveness of Internal Control System

This research examines the internal control system at the bank. The analysis focuses on the control environment, which sets the foundation for effective internal controls throughout the organization. This environment includes the bank's standards, processes, and structures, along with management's commitment to ethical conduct. The findings reveal strengths in both the control environment and control activities, with respondents indicating a strong emphasis on integrity from leadership. This aligns with efforts to address ethical shortcomings within the banking industry.

The research also explores risk assessment, a crucial element of management that helps identify and mitigate potential roadblocks to achieving the bank's goals. While nearly half of the respondents agreed that the bank has a strategy for risk identification and response, some inefficiencies or gaps were identified in this area. Notably, over half of the respondents acknowledged the importance of management's role in risk assessment, which should work hand-in-hand with the internal control team's involvement during operations.

Finally, the research investigates the bank's communication of consequences for illegal activities. The research identified a gap in communication, as 36% of respondents were unaware of or indifferent to the existence of clear systems outlining repercussions for specific actions. This highlights potential weaknesses or gaps in the bank's internal control communication channels.

Table 12: Descriptive statistics of effectiveness of Internal Control System

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Control Environment	57	1	5	3.55	.921
Risk Assessment	57	1	5	2.97	1.084
Control Activity	57	1	5	3.39	1.010
Information & Communication	57	1	5	3.19	.997
Monitoring Activity	57	1	5	3.46	.975
Effectiveness of ICS	57	1.12	4.65	3.31	.72644
Valid N (list wise)	57				

Source: questionnaire and SPSS output (2024)

The survey results indicate a generally positive perception of the bank's internal control system. The average rating of 3.31 suggests that most respondents believe the various components are functioning effectively. In simpler terms, a majority of participants seem to agree that the internal control system within Global Bank Ethiopia S.C. is effective. The relatively high average score (3.31) and low variability (standard deviation of 0.726) indicate that the bank's internal controls are likely functioning effectively.

4.4 Descriptive Statistics

This part explores the characteristics of the variables used in the second conceptual framework, employing descriptive statistics. This research investigated how well different aspects of a bank's internal controls (independent variables) influence how well they detect and prevent fraud (dependent variable). These control aspects include the overall control environment, the thoroughness of risk assessments, and the implementation of control activities, the effectiveness of information and communication channels, and the monitoring activities that take place. Table 13 summarizes the descriptive statistics for all these variables, including measures like average value, highest and lowest values, variation, data distribution (skewness and kurtosis), and the number of observations used in the analysis.

Table 13: Descriptive statistics of variables

Descriptive Statistics

	N	Min	Max	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Control Environment	57	1	5	3.55	.921	-.758	.316	.481	.623
Risk Assessment	57	1	5	2.97	1.084	-.363	.316	-.731	.623
Control Activity	57	1	5	3.39	1.010	-.727	.316	.044	.623
Information & Communication	57	1	5	3.19	.997	-.394	.316	-.495	.623
Monitoring Activity	57	1	5	3.46	.975	-.387	.316	-.525	.623
Fraud Prevention & Detection	57	2	5	2.97	.634	.703	.316	1.295	.623
Valid N (list wise)	57								

Source: questionnaire and SPSS output (2024)

The research analyzed data from 57 participants, measuring six variables. Basic descriptive statistics were used to summarize the overall data. For categorical variables, frequencies and percentages were calculated. The analysis of the independent variables (a strong control environment, thorough risk assessment, implemented control activities, effective information & communication channels, and ongoing monitoring activities) revealed average scores ranging from 2.97 to 3.55, with standard deviations between 0.921 and 1.084. These scores generally fall within the "agree" range on the survey scale. However, the dependent variable, fraud detection and prevention, had an average score of 2.97 (SD=0.634), which falls near the "neutral" point. This suggests a potential gap between perceived effectiveness of internal controls and actual fraud detection and prevention. Interestingly, all variables exhibited consistency, with mean values falling within their maximum and minimum ranges.

4.5 Reliability Analysis

This section addresses the questionnaire's reliability, which gauges the consistency of participants' responses over time (Sekaran, 2003). Reliability is crucial for ensuring the validity of the data gathered. The research employed Cronbach's Alpha using SPSS

version 24.0 for Windows to evaluate the internal consistency of the questionnaire items within each construct. The evaluation criteria for Cronbach's Alpha were based on (George, D., & Mallery, M., 2010), where values exceeding 0.9 indicate excellent reliability, 0.8 to 0.89 indicate good reliability, and so on. As shown in Table 14, the Cronbach's Alpha coefficient for all items was exceptionally high ($\alpha = 0.920$), surpassing the recommended threshold of 0.9 (George, D., & Mallery, M., 2010). This finding suggests that the responses generated for the variables put-upon this research demonstrate excellent internal consistency, making them suitable for further data analysis.

Table 14: Reliability statistics for all items

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.920	.920	6

Source: questionnaire and SPSS output (2024)

The results indicate that the Cronbach's Alpha reliability coefficient for all items is .920, which is considered excellent reliability. This means that the set of items used to measure a particular concept is highly consistent internally. In other words, the items are all measuring the same underlying construct in a very similar way.

Table 15: Reliability statistics for control environment

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.730	.719	5

Source: questionnaire and SPSS output (2024)

This indicates acceptable reliability. While not excellent, it suggests there's a decent level of internal consistency within these 5 items.

Table 16: Reliability statistics for risk assessment

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.716	.696	5

Source: questionnaire and SPSS output (2024)

This falls on the borderline between acceptable reliability and questionable reliability. It means the items have some internal consistency, but it could be improved.

Table 17: Reliability statistics for control activities

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.738	.724	5

Source: questionnaire and SPSS output (2024)

Similar to the first set, this shows acceptable reliability. There's a decent level of consistency within these 5 items.

Table 18: Reliability statistics for information and communication

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.733	.751	4

Source: questionnaire and SPSS output (2024)

This is again in the range of acceptable reliability. Even though there are only 4 items, they show a decent level of internal consistency.

Table 19: Reliability statistics for monitoring activity

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.796	.800	4

Source: questionnaire and SPSS output (2024)

This is the highest value and falls within the range of good reliability. These 4 items demonstrate a strong level of internal consistency.

4.6 Correlation Analysis

This section investigates how different control practices (independent variables) influence fraud detection and prevention (the dependent variable) within Global Bank Ethiopia S.C. These control practices include: a strong control environment, thorough risk assessments, implemented control activities, effective information & communication channels, and ongoing monitoring activities. Pearson correlation coefficients will be employed to measure the strength and direction of the relationships between these variables. The specific findings of this analysis are presented in Table 20.

Table 20: Correlation matrix (with dependent variable)

Correlations

		Effectiveness Control Environment	Effective Risk Assessment	Effective Control Activity	Effective Information & Communication	Effective Monitoring Activity	Fraud Prevention & Detection
Effectiveness Control Environment	Pearson Correlation	1					
	Sig. (2-tailed)						
Effective Risk Assessment	Pearson Correlation	.421**	1				
	Sig. (2-tailed)	.001					
Effective Control Activity	Pearson Correlation	.543**	.530**	1			
	Sig. (2-tailed)	.000	.000				
Effective Information & Communication	Pearson Correlation	.357**	.125	.527**	1		
	Sig. (2-tailed)	.006	.356	.000			
Effective Monitoring Activity	Pearson Correlation	.456**	.237	.367**	.600**	1	
	Sig. (2-tailed)	.000	.076	.005	.000		
Fraud Prevention & Detection	Pearson Correlation	.224	-.294*	-.068	.475**	.528**	1
	Sig. (2-tailed)	.094	.027	.616	.000	.000	
	N	57	57	57	57	57	57

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: questionnaire and SPSS output (2024)

Table 20 presents the correlation matrix, a statistical tool that reveals the degree of association between variables (Gujarati, 2004). Correlation coefficients measure the strength and direction of linear relationships among variables. As noted by (Gujarati, 2004), these coefficients range from +1 (indicating a perfect positive correlation) to -1 (indicating a perfect negative correlation). A statistically significant correlation coefficient suggests a meaningful relationship, and the sample size plays a crucial role in determining this significance.

The analysis in Table 20 reveals that the correlations among the control aspects (independent variables) and fraud detection/prevention (dependent variable) were generally moderate. The strongest positive correlation (0.528, significant at the 0.01

level) exists between fraud detection/prevention and effective monitoring activities. This suggests a potentially important link between strong monitoring and successful fraud detection/prevention within Global Bank Ethiopia S.C.'s internal control system (ICS). The correlation between fraud detection/prevention and effective information & communication is the second highest (0.475, significant at the 0.01 level), indicating another potentially valuable association.

Effective control activities, effective risk assessment, and effective control environment have weaker correlations with fraud detection/prevention (0.224, 0.294, and 0.068 respectively, all significant at the 0.05 level). While these correlations are statistically significant, their lower values suggest a less pronounced relationship compared to monitoring and communication.

4.7 Econometric Analysis

To ascertain the reliability of the regression analysis, the author employed diagnostic tests to identify and address potential issues that could lead to misleading outcome. The findings of these tests are presented in the next sections.

4.7.1 Multicollinearity Test

This section examines the correlations among the independent variables to assess the potential presence of multicollinearity. The correlation matrix, presented in the next table, will reveal if any independent variables exhibit excessively strong linear relationships that could affect the regression analysis.

Table 21: Correlation matrix (only independent variables)

Correlations

		Effectiveness Control Environment	Effective Risk Assessment	Effective Control Activity	Effective Information & Communication	Effective Monitoring Activity
Effective Control Environment	Pearson Correlation	1				
	Sig. (2-tailed)					
Effective Risk Assessment	Pearson Correlation	.421**	1			
	Sig. (2-tailed)	.001				
Effective Control Activity	Pearson Correlation	.543**	.530**	1		
	Sig. (2-tailed)	.000	.000			
Effective Information & Communication	Pearson Correlation	.357**	.125	.527**	1	
	Sig. (2-tailed)	.006	.356	.000		
Effective Monitoring Activity	Pearson Correlation	.456**	.237	.367**	.600**	1
	Sig. (2-tailed)	.000	.076	.005	.000	
	N	57	57	57	57	57

**. Correlation is significant at the 0.01 level (2-tailed).

Source: questionnaire and SPSS output (2024)

Multicollinearity, a situation where independent variables are highly correlated, can pose a problem for regression analysis (Gujarati, 2004). As (Gujarati, 2004) suggests, correlations exceeding 0.8 or falling outside the -0.8 to 0.8 range are typically considered problematic. Examining the correlation matrix presented earlier, the author can see that no pair of independent variables exhibits a correlation coefficient above 0.8. This suggests that the author can fail to reject the null hypothesis (H_0), which states that there are no excessively strong linear relationships between the independent variables. The highest correlation observed in the table is 0.600, between effective monitoring activities and effective information & communication.

According to (Cooper, D. R., & Schendlar, R. Z., 2009), the absence of correlations exceeding 0.8 indicates that multicollinearity is not a significant concern in this research. Therefore, the regression analysis can be considered reliable as multicollinearity does not appear to be an issue. In conclusion, the variables used in the model can be retained for further analysis without concerns about multicollinearity.

4.7.2 Linearity Test

Linearity is an important assumption in regression analysis. It refers to the idea that alter in the independent variables are correlated with consistent changes in the dependent variable. In this research, the focus is on whether the relationship between fraud detection/prevention (dependent variable) and the control aspects (independent variables): a strong control environment, thorough risk assessment, implemented control activities, information & communication, and monitoring activities is linear. To assess this, the residuals from the regression analysis were plotted using SPSS software.

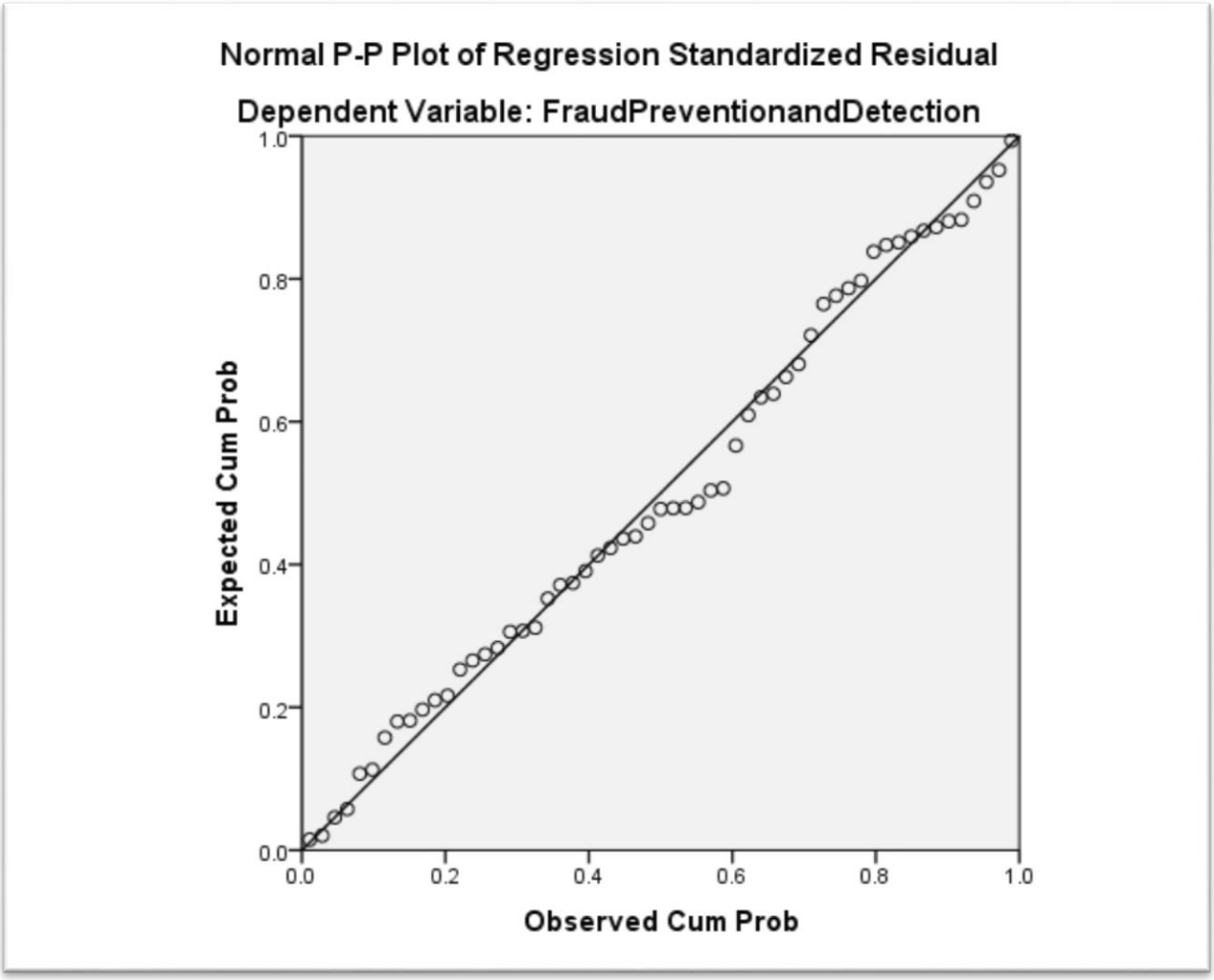

Figure 2: Normal point plot of standardize residual

Source: questionnaire and SPSS output (2024)

Figure 2 displays the distribution of the residuals from the regression analysis. The scatter plot shows a relatively consistent spread of the residuals across the x-axis, suggesting a linear relationship between the independent variables and the dependent variable. Additionally, the figure visually indicates that the residuals are normally distributed around a mean of zero. This normality assumption is crucial for ensuring the validity of the inferences drawn about the population parameters based on the sample data.

4.7.3 Normality Test

Figure 3 shows how the standardized residuals are spread out compared to a normal bell curve. While some residuals (like those near zero) deviate slightly from the normal curve, the majority fall fairly close. Additionally, the histogram's bell shape suggests that the residuals (errors) are generally normally distributed. This adherence to the normality assumption of the error terms strengthens the validity of the regression analysis.

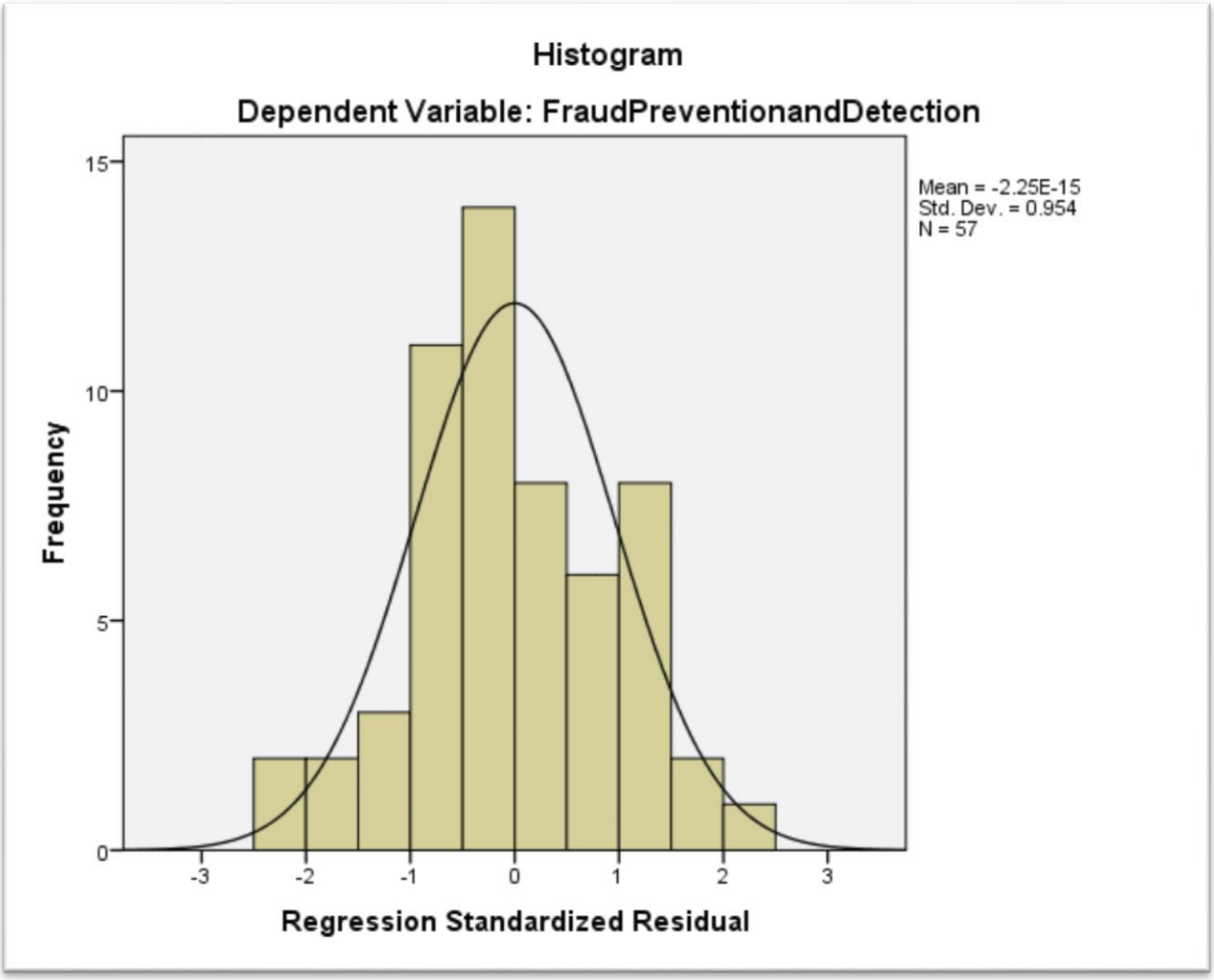

Figure 3 : Frequency distribution of standardized residual

Source: questionnaire and SPSS output (2024)

Based on the analysis of the various tests conducted (refer to previous sections for details), the researcher has not identified any major data issues that would significantly violate the core assumptions of classical linear regression. This suggests that the

regression model is likely reliable and the results can be interpreted with more confidence.

4.8 Regression Analysis

This research employed regression analysis to investigate how control systems within Global Bank Ethiopia S.C. influence and predict fraud detection and prevention.

The research tested the following hypotheses:

Ha1: A strong ethical culture within Global Bank Ethiopia S.C, fostered by management commitment and effective communication of control policies, contributes significantly to the effectiveness of the bank's internal control system in preventing and detecting fraudulent activities (COSO, 2013).

Ha2: A comprehensive and ongoing risk assessment process that identifies and prioritizes fraud risks specific to the Ethiopian banking sector allows Global Bank Ethiopia S.C to implement targeted control activities that effectively mitigate those risks (COSO, 2013).

Ha3: The design and implementation of a robust set of control activities, aligned with identified fraud risks, significantly reduces the bank's exposure to fraudulent activities (COSO, 2013).

Ha4: Effective communication of control policies, procedures, and identified fraud risks throughout all levels of the bank empowers employees to recognize and report suspicious activities, leading to improved fraud detection (COSO, 2013).

Ha5: Regular and independent monitoring activities that assess the ongoing effectiveness of the internal control system in response to evolving fraud risks enable Global Bank Ethiopia S.C to identify and address control weaknesses promptly, preventing future fraudulent activities (COSO, 2013).

The hypotheses outlined earlier were examined statistically using a regression model. This model, presented below, is the operational linear regression equation used to assess the statistically significant relationships between fraud prevention & detection (FPD) and the various internal control components within Global Bank Ethiopia S.C.

$$FPD = \alpha i + \beta 1 * CE + \beta 2 * RA + \beta 3 * CA + \beta 4 * IC + \beta 5 * MA + \varepsilon \dots\dots\dots (4.1)$$

The equation breaks down the factors influencing fraud prevention and detection (FPD) within Global Bank Ethiopia S.C. The variables X_1 to X_5 ($\beta 1, \beta 2, \beta 3, \beta 4\ and\ \beta 5$) represent the different components of the bank's internal control system: control environment, risk assessment, control activities, information & communication, and monitoring activities. Together, these components contribute to the overall effectiveness of fraud prevention and detection, symbolized by Y. control environment, risk assessment, control activities, information & communication and monitoring activities as components of internal control respectively and Y represent indicators of fraud prevention & detection (FPD).

4.8.1. Overall regression model and its ANOVA

A) Regression model summery

The regression analysis results are presented below.

Table 22: Regression model Summery

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.759	.576	.534	.433	1.481

a. Predictors: (Constant), Effective Monitoring Activity, Effective Risk Assessment, Effective Control Environment, Effective Information and Communication, Effective Control Activity
b. Dependent Variable: Fraud Prevention and Detection

Source: questionnaire and SPSS output (2024)

The statistical model demonstrates a good fit, explaining roughly 76% of the variance in the dependent variable. The adjusted R-squared value of 0.534 indicates this explanatory power is achieved without excessive over fitting to the data. Additionally, the Durbin-Watson statistic of 1.481 suggests no major concerns with autocorrelation in the model's residuals. The analysis (refer to Table 22) revealed that the model's explanatory variables account for approximately 53.4% of the variation in Global Bank Ethiopia S.C.'s fraud prevention and detection levels. This means there are other, unaccounted-for factors influencing the remaining 46.6% of the variation.

B) Analysis of Variance

To examine how internal controls affect fraud prevention and detection in Ethiopian banks, this research employed a statistical technique called analysis of variance. The results of this analysis are presented below.

Table 23: Regression-ANOVA

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.986	5	2.597	13.858	.000[b]
	Residual	9.558	51	.187		
	Total	22.544	56			

a. Dependent Variable: Fraud_Prevention_and_Detection

b. Predictors: (Constant), Effective_Monitoring_Activity, Effective_Risk_Assessment, Effectiveness_Control_Environment, Effective_Information_and_Communication, Effective_Control_Activity

Source: questionnaire and SPSS output (2024)

Table 23 shows a statistically significant relationship (p-value < 0.01) between the internal control components (a strong control environment, thorough risk assessment, implemented control activities, effective information & communication channels, and ongoing monitoring activities) and the level of fraud prevention and detection (FPD) in Ethiopian banks. This suggests that these internal control components significantly

contribute to better FPD. However, the strength of this influence might vary for each component.

Further analysis using linear regression (not shown) indicates that the impact of FPD on each internal control component differs. While the overall model is statistically significant (p-value = 0.000), suggesting a good fit, we can't assume all internal control components are equally affected by FPD.

C) Test for Coefficients

This table summarizes the significance levels of the variables in the model. Additionally, it presents both the standardized and unstandardized coefficients for each variable.

Table 24: Regression Coefficient Analysis of the Model

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	2.068	.275		7.526	.000		
	Effective Control Environment	.172	.081	.250	2.136	.038	.608	1.645
	Effective Risk Assessment	-.203	.067	-.346	-3.043	.004	.642	1.558
	Effective Control Activity	-.231	.085	-.368	-2.712	.009	.452	2.214
	Effective Information & Communication	.243	.083	.381	2.919	.005	.488	2.049
	Effective Monitoring Activity	.262	.079	.402	3.298	.002	.558	1.791

a. Dependent Variable: Fraud Prevention and Detection

Source: questionnaire and SPSS output (2024)

The data in Table 24 was used to investigate how internal controls affect fraud prevention and detection at Global Bank Ethiopia S.C. This analysis resulted in the following regression equation:

$$FBD = 2.068 + 0.172 * CE - 0.203 * RA - 0.231 * CA + 0.243 * IC + 0.262 * MA + \varepsilon \dots\dots\dots (4.2)$$

This analysis assumes all other factors remain unchanged. It shows that the effectiveness of fraud prevention and detection at Global Bank Ethiopia S.C. is directly linked to how well internal controls are designed and implemented. The detailed results of this multiple regression analysis are presented in the next section.

4.9. Discussion and Interpretation of Findings

I. Strong Control Environment (CE) Vs. Fraud Prevention & Detection (FPD)

The analysis revealed a positive coefficient for the control environment variable, indicating a beneficial effect on FPD. There's a positive relationship between the control environment and fraud prevention/detection. Specifically, an increase of one unit in the control environment score is linked to a 0.172 unit increase in the FPD score, holding all other variables constant. This positive association is statistically significant, with a p-value of 0.038, which is well below the commonly accepted threshold of 0.05. Stated simply, strong control environments have a significant positive impact on FPD within the Global Bank Ethiopia S.C. Based on the results, the researcher can dismiss the idea (null hypothesis) that there's no connection between the control environment and fraud prevention/detection (FPD) at Global Bank Ethiopia S.C. Instead, the findings support the opposing view (alternative hypothesis) - there's a clear and positive relationship between a strong control environment and better FPD. These findings align with prior research by (Mawanda, 2008), who identified a positive association between control environment and FPD. This suggests that the control environments implemented by Global Bank Ethiopia S.C are effective in mitigating fraud.

II. Thorough Risk Assessment (RA) Vs. Fraud Prevention & Detection (FPD)

The research found an interesting link between risk assessment and fraud prevention at Global Bank Ethiopia S.C. Surprisingly, there seems to be a negative association. This means banks with more comprehensive risk assessments (higher scores) tend to have slightly lower fraud prevention scores (FPD). On average, for every unit increase in risk assessment score (assuming other factors are constant), FPD scores decrease by 0.203.

However, this relationship is statistically significant (p-value = 0.004), meaning it's unlikely due to chance.

In simpler terms, even though the results seem counterintuitive, they confirm that risk assessment significantly impacts fraud prevention at the bank. We can therefore reject the idea that there's no connection between these two aspects. This suggests the bank's risk assessment practices are effective in controlling fraud. This finding supports what other researchers have observed. For instance, Tunji's research in 2013 showed that having strong risk assessments in place can lead to fewer financial issues caused by fraud within banks.

III. Control Activity (CA) Vs. Fraud Prevention & Detection (FPD)

Interestingly, the analysis for Global Bank Ethiopia S.C. revealed a negative association between control activities and fraud prevention. This means that banks with a higher level of control activities (higher score) tend to have slightly lower fraud prevention scores (FPD). On average, an increase of one-unit in control activity score (assuming other factors are constant), FPD scores decrease by 0.231. However, this negative relationship is statistically significant (p-value = 0.009), indicating it's not likely due to chance.

In simpler terms, while the results appear counterintuitive, they confirm that control activities significantly impact fraud prevention at the bank. We can therefore reject the idea of no connection between these aspects. This suggests that the bank's current control activities might be identifying and preventing fraud so effectively that there are fewer instances to detect. This aligns with the concept of well-designed controls reducing opportunities for fraud.

IV. Effective Information & Communication (IC) Channels Vs. Fraud Prevention & Detection (FPD)

The research revealed a positive connection between how well information flows within the bank (information and communication systems) and their ability to prevent fraud (FPD). In other words, banks with clear and effective communication channels tend to

have better scores in fraud prevention. The research found that strengthening a bank's information and communication systems by one unit is associated with an average increase of FPD scores increase by 0.243 on average. This suggests that clear and effective communication channels can play a significant role in preventing fraud. Importantly, this positive relationship is statistically significant (p-value = 0.005), meaning it's unlikely due to chance.

In simpler terms, these findings clearly demonstrate that well-established information and communication systems significantly contribute to a bank's ability to prevent fraud. We can therefore reject the idea that there's no connection between these aspects. This aligns with research by Tunji (2013) who highlighted the importance of timely and accessible information sharing in preventing financial fraud.

V. Ongoing Monitoring Activities (MA) Vs. Fraud Prevention & Detection (FPD)

The research revealed a clear connection between how well a bank monitors its activities (monitoring activities) and its success in preventing and identifying fraud (FPD). This link is statistically significant, with a coefficient of 0.262 and a very low p-value of 0.002 (well below the standard threshold of 0.05). In simpler terms, for every unit a bank improves its monitoring practices (assuming all other factors are constant), their fraud prevention and detection scores increase by an average of 0.262. This statistically significant association suggests that stronger monitoring activities are a positive predictor of higher FPD levels within the bank. We can therefore reject the idea of no connection between monitoring and FPD. These findings align with the International Federation of Accountants ((IFAC)., 2012), who emphasize the critical role of monitoring as a component of internal control systems (ICS). When implemented effectively, monitoring can help detect errors or fraudulent activities early on, mitigating potential harm to the organization ((IFAC)., 2012).

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Introduction

Building upon the examination of Internal Control Systems (ICS) effectiveness in preventing and detecting fraud within Global Bank Ethiopia S.C (GBE) presented in the preceding chapter, this chapter condenses the key findings, draws conclusions, and proposes actionable recommendations.

5.2 Summary of the Research and Major Findings

This research examined how well Global Bank Ethiopia's internal controls work to prevent and catch fraud. The researcher used a framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) to assess five key areas: the overall control environment, how well risks are identified (risk assessment), the specific controls in place (control activities), how information is shared (information and communication), and how controls are monitored over time (monitoring activities). Finally, the researcher used a statistical method called regression analysis to see how these different control components are linked to the bank's success in preventing and detecting fraud (FPD).

- Questionnaires were used to gather data from a sample of employees across various experience levels within 57 East District Addis Ababa branches. Statistical analysis (descriptive statistics and multiple regressions) was conducted using SPSS software.
- The findings suggest that employees generally agreed that all five components of ICS (control environment, risk assessment, control activities, information & communication, and monitoring activities) are effective in controlling fraud.
- The correlation analysis indicated no significant multicollinearity (highest at 0.6) among the variables, ensuring the reliability of the regression analysis.

- The research established a statistically significant relationship between overall ICS and FPD. ANOVA tests confirmed a significant joint influence of all ICS components on FPD.
- The model explained a substantial proportion (adjusted R-squared = 53.4%) of the variation in FPD. The analysis revealed a positive relationship between three ICS components (control environment, information & communication, and monitoring activities) and FPD. However, the impact of risk assessment and control activities was not statistically significant.
- A strong control environment, with a focus on ethical culture and communication of control policies, has a positive impact on FPD.
- Risk assessment plays a significant role in FPD, with comprehensive assessments leading to more effective control measures.
- Control activities also have a significant positive impact on FPD.
- Effective information and communication systems are crucial for fraud prevention and detection.
- Regular and robust monitoring activities are essential for maintaining the effectiveness of the internal control system and identifying control weaknesses that could lead to fraud.

These findings suggest that a well-designed and implemented internal control system, particularly with a strong control environment, effective communication, and robust monitoring activities, can significantly enhance fraud prevention and detection capabilities in Global Bank Ethiopia S.C.

5.3 Conclusions

Based on the analysis, the author can conclude that... The research yielded the following key conclusions:

- Poor internal control system, presence of unqualified staff, greed on the part of employees inadequate staffing, poor record-keeping practices, and inadequate training and re-training of staff among others were identified as the main causes of fraud in the selected bank.

- Based on the findings of the research, it is concluded that the effective internal control system (ICS) established by the bank is able to control fraud as supported by the research findings on control environment, risk assessment, control activities, information & communication and monitoring.

- A strong control environment within GBE has a significant positive impact on FPD, aligning with expectations and prior research. This highlights the importance of fostering a culture of integrity and ethical conduct within the bank.

- Interestingly, the analysis revealed negative but statistically significant relationships between risk assessment, control activities, and FPD. However, these findings can be interpreted positively. They suggest that GBE's risk assessment and control activities are likely effective in preventing fraud, leading to fewer instances to detect. This emphasizes the importance of designing preventive controls that reduce opportunities for fraud.

- Effective information and communication channels emerged as a significant positive predictor of FPD. This underscores the critical role of clear communication in empowering employees to identify and report suspicious activities.

- Consistent with established best practices, the research found a strong positive correlation between monitoring activities and FPD. This reinforces the importance of ongoing monitoring to detect and address control weaknesses promptly.

These findings support the COSO framework and its importance in establishing a strong internal control system to mitigate fraud risk.

5.4 Recommendations

The following recommendations stem from the research findings for Global Bank Ethiopia S.C.

- GBE should continue to prioritize fostering a strong control environment that emphasizes ethical conduct and compliance.
- The bank's risk assessment and control activities should be reviewed to ensure they remain aligned with evolving fraud risks. While the negative coefficients suggest effectiveness in prevention, further analysis could explore if these processes can be optimized to also improve detection capabilities.
- The importance of clear and open communication throughout the bank should be emphasized. This can be achieved through training programs and fostering a culture where employees feel comfortable reporting suspicious activities.
- GBE should continue to invest in robust and ongoing monitoring activities. This allows for the timely identification and rectification of control weaknesses, ultimately strengthening the bank's defense against fraud.
- Regarding to causes of fraud in the bank, it is recommended that the bank should consider eliminating poor internal control system, unqualified staff, inadequate staffing, poor record-keeping practices, and inadequate training and re-training of staff among others through frequent supervision. Training and re-training programs can be organized for employees regarding the practices of internal control system.
- The research further recommends that the governing body, possibly supported by the audit committee, should ensure that the internal control system is periodically monitored and evaluated. The actual assessment can be executed by the organization‘s management. A staff person who is sufficiently independent from those responsible for the system, such as the internal auditor, could provide additional assurance on the effectiveness and cost efficiency of the internal control system. The bank should transparently report on the structure and performance of their internal control system in their various reports to internal and

external stakeholders, such as through their periodic accountability reports or on the organization‘s website.

By implementing these recommendations and considering the broader context, GBE can continue to strengthen its internal control system and enhance its ability to prevent and detect fraud. This will contribute to a more secure and ethical banking environment for GBE and its stakeholders.

References

(ACFE)., A. o. (2008). *Report to the nations on occupational fraud and abuse.* Austin, TX: ACFE.

(AFE)., A. o. (2016). *Anti-Fraud Policy & Procedures Guide.* . Austin, : TX: AFE.

(AICPA)., A. I. (2016). *The AICPA Professional Ethics Code.*

(COSO)., C. o. (2013). *Internal Control – Integrated Framework.* Jersey City,: NJ: COSO.

(IFAC)., I. F. (2012). *International Standard on Auditing (ISA) 500:* . Audit Evidence.

Adams, C. E., & McNair, M. S. (2018). Internal controls and financial reporting: . *A literature review. Accounting Horizons,* , 32(2), 409-434.

Adams, C. E., & McNair, M. S. (2018). *Internal controls and financial reporting: A literature review. Accounting Horizons, 32(2), 409-434.*

Akinyemi, O. O., & Adegboye, O. A. (2023). The impact of technological advancements on internal control systems and fraud prevention in the banking industry: A study of selected commercial banks in Nigeria. . *Journal of Risk Management, 16(1),* , 1-18.

Albrecht, W. Steve, Robert J. Albrecht, and Marvin S. Romney. (1993:). "Fraud tree: A tool for fraud prevention and detection." . *Auditing: A Journal of Practice & Theory 12.2* , 1-17.

Alemayehu, G. (2016). Assessment of Internal Control System: A Case of Development Bank of Ethiopia. .

Al-Zubi, M. A., & Habib, K. A. (2019). The moderating role of ethical culture on the relationship between internal control systems and fraud prevention in Islamic banks. *International Journal of Accounting and Economics, 26(2),* , 117-135.

Anjali, V. E., Amuda, O. O., & Arulogun, O. A. (2013). An Examination of the Effectiveness of Internal Control Systems in Preventing Fraud in the Nigerian Banking Sector. .

Ashenafi. (2017). Assessments of Internal Control System in a Selected Microfinance Institution. .

Association of Certified Fraud Examiners (ACFE). (2018). *Report to the nations on occupational fraud and abuse.*

Attwood, F. A. & Stein, N. D. (1986). Bank Frauds: A Look at the Nigerian Banking Clearing System, ICAN News, January/March,. In P. E. Asukwo, *Auditing (17th ed.).* (pp. pp 19-24.). Pitman Publishing Ltd.

Atuk, O. E. (2011). Evaluating the effectiveness of internal control systems in Nigerian banks. .

Ayagre, W., Darkwah, N. A., & Adusei, M. (2014). Evaluating the effectiveness of the control environment and monitoring activities components of internal control systems of Ghanaian banks. . *International Journal of Finance and Accounting,* , 4(2), 121-130.

Bandura, Albert. (1977.). *Social learning theory.* . Prentice Hall, .

Beck, T., & Levine, R. (2004). Financial institutions and growth in developing economies. . *Handbook of economic growth,*, 1(1), 727-804.

Clarke, Ronald V. (1997). *"Opportunity makes the thief: Crime and crime prevention in the opportunity structure."*. Rutgers University, Center for Crime Prevention Research.

Cohen, Lawrence E., and Marcus Felson. (1979). "Social change and crime rate trends: A routine activity approach.". *American sociological review*, 488-503.

Cooper, D. R., & Schendlar, R. Z. (2009). *Business research methods (10th ed.).* McGraw-Hill.

Cornish, Derek B., and Ronald V. Clarke. (1986). *"Rational choice theory and crime control: Implementing a decision theory model."*.

COSO. (2013). Internal Control — Integrated Framework Executive Summary.

COSO. (1992). *internal control-integrated framework.* Retrieved july 10, 2012, from Available: http://www.coso.org/publications/executive_

COSO. (2013, May 25,). *Internal Control Issues in Derivatives Usage.* Retrieved from Retrieved from http://www.aicpa.org/Ic-Issues-Derivatives: http://www.aicpa.org/Ic

Cressey, D. (1973). Other People's Money: A Study in the Social Psychology of Embezzlement. . *Montclair, NJ: Patterson-Smith.* .

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement.* . Glencoe, IL: Free Press.

Cressey, D. R. (1953.). *Other people's money: A study in the social psychology of embezzlement.* . Free Press, .

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.).* . Sage Publications. .

David Ingram. (2019). What Are the Seven Internal Control Procedures in Accounting?

De Vaus, D. A. (2002). *Surveys in social research (5th ed.).* . Routledge.

Denzin, N. K. (2017). *Research methods in social sciences (12th ed.).* . Sage Publications.

Dinapoli, A. (2005). *Internal control systems.* . John Wiley & Sons.

Douglas, N. (2011). Internal Control and its Contributions to Organizational Efficiency and Effectiveness:. *A case Study of Eco bank Ghana limited. Retrieved from http://ir.knust.edu.gh/bitstream/123456789/4210/1/Douglas%20thesis.pdf.* .

Eisenhardt, Kathleen M. (1989:). "Agency theory: An assessment and review." . *Academy of management review 14.1*, 57-74.

Examiners, A. o., & (ACFE). (2018). *A Fraud Risk Assessment Guide.* Austin,: TX: ACFE.

Fikru Worku. (2018). Internal control systems and their effectiveness in preventing fraud in banks: The case of Ethiopia. *African Journal of Accounting and Economics Management, 4(1),*, 1-15.

Geiger, M. .. (2004). Internal control components: Did COSO get it right? *The CPA Journal, 7(1)*, 28-31.

George, D., & Mallery, M. (2010). *SPSS for Windows step by step: A simple guide and reference.* . Allyn & Bacon.

Gibbs, John J., and Alfred Henry Finch. (2012:). "Toward a theoretical integration of psychological and sociological explanations of criminal behavior." . *Criminology 50.4*, 763-791.

Gujarati, D. N. (2004). *Basic econometrics (4th ed.).* . McGraw-Hill.

Howard, M. (1984). Internal control in the modern business environment. . *Accounting Horizons,* , 18(2), 123-132.

Idowu, S. O., & Adedoku, A. O. (2013). The impact of internal control systems on fraud risk in Nigerian banks. . *Journal of Money Laundering Control,* , 16(2), 182-190.

IIA. (2017). Effect of internal controls on fraud the detection and prevention among commercial banks in Kenya. *European Journal of Business and Strategic Management. ISSN 2518-265X (Online) Vol.2, Issue 1 No.4,*, pp 52- 68, 2017.

Institute of Internal Auditors. (2023). *Internal Controls – Integrated Framework (ICIF).* Retrieved from https://www.theiia.org/

International Federation of Accountants (IFAC). (2012). *Internal Control – Applying the Framework (IAASB Practice Note).*

International Monetary Fund (IMF). (2009). *Internal Control Guidance for Public Financial Management.* . Retrieved from https://ofm.wa.gov/policy/20.15.pdf

INTOSAI. (2001). *Frame of internal control system.* International Organisation of Supreme Auditing Institutions.

Jenkinson, N. (2008). *Strengthening Regimes for Controlling Liquidity Risks: Some Lessons from the Recent Turmoil.* .

Joseph, A., Albert, L., & Byaruhanga, E. (2012). The Impact of Internal Controls on Fraud Detection and Prevention in District Treasuries of Kakamega County, Kenya.

Kinney, W. (2000). Research opportunities in internal control quality and quality assurance. *Auditing: A Journal of Practice & Theory*,(19), 83-90.

Kothari, C. (2004). *Research Methodology: Methods and Techniques.* . New Age International Publishers.

Lacotelli, G. (2009). *A guide to internal controls.* Harvard University.

Lamoye. (2005). Internal Controls and Cost. . *NF Perspective Journal*, pp 4.

Leah N., & Dr. Josiah A. (2017). Impact of internal control systems on fraud prevention in commercial banks in Kenya. *International Journal of Economics and Finance, 9(8),* , 1-10.

Levine, R. (1991). Financial markets and economic growth. . *The American Economic Review,*, 81(4), 888-907.

Lousteau, E. (2006). *Internal controls: An integrated approach.* . Pearson Education.

Martin, A. (2010). Risk Assessments Pay Forward,. *Risk Response and Reduction in Internal Auditing.*, 12-26.

Mawanda, E. (2008). The impact of internal control environment on fraud prevention and detection in a developing economy.

McKinsey & Company. (2016). *Unlocking Productivity: A Renewed Vision for Financial Institutions in Africa.* . Retrieved from https://www.mckinsey.com/

Millichamp, A. (2002, june 7). *Internal Control Policy [online] available at*. Retrieved from Auditing (8th Ed.). London: Thomson Learning Queensland University of Technology (2005); Manual of Policies and Procedures:: http://www.mopp.qut.edu.au/ contact.jsp

Millichamp, A. H. (2002). *Internal control systems.* . Palgrave Macmillan.

Millichamp, A.H. (2002, june 7). *Internal Control Policy [online] available at*. Retrieved from Auditing (8th Ed.). London: Thomson Learning Queensland University of Technology (2005);: http://www.mopp.qut. edu.au/ contact.jsp [accessed 7 June 2012]

Mishkin, F. S. (2007). *The monetary transmission mechanism (Vol. 2).* . MIT press.

Muhota, K. (2005). *Check list for an internal Audit.* USA.: Giving hope to world of need.

Owizy, I. N., & Uadiale, M. O. (2013). The effectiveness of internal control systems in detecting and preventing fraud in banks in Nigeria. . *Journal of Risk Management, 4(2),* , 114-128.

Pany, O. Ray Whittington & Kurt. (2001). *Principles of auditing and other assurance services.* New York.: Irwin/McGraw- Hill.

PwC. (2019). *Global Economic Crime Survey 2019: Key findings for the financial services sector.*

Rae., K. S. (2006). *The Relationship between Internal Control Procedural Quality, Organizational Justice Perceptions and Employee Fraud.* Multimedia, Malaysia:: Multimedia University press.

Ramos, M. (2004). Evaluate the Control Environment: Documentation Is Only a Start; now it's all about asking questions. *Journal of Accounting,*, 75 - 79.

Ramos, M. (2004). Evaluate the Control Environment: Documentation Is Only a Start; now it's all about asking questions. . *Journal of Accounting*, 75 - 79.

Rea, L. M., & Parker, R. A. . (2014). *Designing and conducting social research (5th ed.).* . Wiley-Blackwell.

Rezaee, Z. (2002). The role of internal control system in enhancing accountability and performance in organizations. . *Management Science,*, 48(8), 1034-1047.

Rittenberg, L. L. (2007).

Sarbanes-Oxley Act of 2002,. (2002). Pub. L. No. 116 . *Stat. 747* , 107-204,.

Sekaran, U. (2003). *Research methods for business: A skill-building approach (4th ed.).* . John Wiley & Sons.

Simmons, J. E. (1995).

Smith, J. (2023). *Internal control systems: A response to financial scandals.* . ABC Press.

Tekalegn. (2019). Assessing the Effectiveness of the Internal Control System in the Commercial Bank of Ethiopia: A Case of Hawassa City.

Teshome, A., & Kebede, G. . (2020). The effectiveness of internal control systems in preventing fraud in Ethiopian banks. . *African Journal of Business Management, 14(8),* , 112-123.

Watts, R. L., & Zimmerman, J. L. (1986). *Positive accounting theory.* . Prentice-Hall.

Wells, J. T. (2006). *Fraud examination.*

Woldie, M. (2023). Challenges in fraud risk management in Ethiopian banks: An analysis of internal control weaknesses. . *Journal of Financial Crime Investigation, 10(1),* , 45-58.

Wolfe, D. T., & Beaumaris, A. L. (2007). The occupational fraud triangle revisited. *Journal of Occupational Fraud Investigation, 25(4), 14-22.*

World Bank. (2023). *Ethiopia Economic Update [Report]*.

World Bank. . (2017). *Curbing corruption: An international handbook.*

Annex

Questionnaires' For the Assessment of the Effectiveness of Internal Control System in Detection and Prevention of Fraud in Global Bank Ethiopia

Thank you for participating in this important research on the effectiveness of Global Bank Ethiopia's internal control system (ICS) in preventing and detecting fraud. Your responses will be anonymous and confidential.

- Demographic information

1 Sex Male ☐ Female ☐

2 Age 20 – 27 yrs. ☐ 28 – 35 yrs. ☐ 36 – 42yrs ☐ 43 – 50yrs ☐ Above 50 ☐

3 Education Diploma ☐ B.A ☐ M.A/M.S.C ☐ PHD ☐

4 Year of service in the bank 1 –5yrs. ☐ 6 – 10 yrs. ☐ 11 – 15 yrs. ☐ 16 – 20 yrs. ☐ 21yrs. &above ☐

5 Which location do you work at? Branch ☐ Head office ☐

6 What is your job title/position? _____

Part1. Internal control system (ICS) awareness and implementation

- Please indicate by **(√)** your level of agreement with the following statements using a scale of 1 to 5. Here, 1 represents "Strongly Disagree," 2 represents "Disagree," 3 represents "Neutral," 4 represents "Agree," and 5 represents "Strongly Agree."

S.N	**1. Control Environment**	**1**	**2**	**3**	**4**	**5**
1	The bank promotes a strong ethical culture that emphasizes honesty and integrity.					
2	Management demonstrates a clear commitment to preventing and detecting fraud.					
3	There are formal written policies and procedures for internal control activities.					

4	Employees are adequately trained on fraud risks and control procedures.					
	2. Risk Assessment					
5	The bank regularly identifies and assesses the potential fraud risks it faces.					
6	The risk assessment process is comprehensive and considers all relevant factors.					
7	The identified fraud risks are prioritized based on their severity and likelihood.					
8	Appropriate controls are implemented to mitigate the identified fraud risks.					
	3. Control Activities					
9	The bank has implemented effective controls over key financial processes.					
10	Controls are designed to prevent unauthorized access to assets and records.					
11	There is adequate segregation of duties to prevent fraud and errors.					
12	Transactions are regularly monitored and reconciled to identify discrepancies.					
	4. Information and Communication					
13	Relevant information about fraud risks and control procedures is effectively communicated to all employees.					
14	There are open channels for employees to report suspected fraud without fear of retaliation.					

15	Management regularly reviews and updates internal control documentation.					
	5. Monitoring Activities					
16	The bank actively monitors the effectiveness of its internal control system.					
17	Internal audits are conducted regularly and address all relevant control areas.					
18	Management takes timely action to address any identified weaknesses in the internal control system.					

Part 2: Fraud Prevention and Detection

- Please indicate your perception of the following aspects of fraud prevention and detection at Global Bank Ethiopia:

19 How effective are the current internal controls in preventing fraud?

- Not effective at all
- Somewhat effective
- Moderately effective
- Very effective
- Extremely effective

20 How confident are you that the bank would be able to detect fraud if it occurred?

- Not confident at all
- Somewhat confident
- Moderately confident

- Very confident
- Extremely confident

21. Have you ever personally observed or suspected fraudulent activity at the bank?
- Yes
- No

22. If you answered yes to the previous question, please briefly describe the suspected activity._____
_____
____

23. How well do you agree that the current regulatory environment in Ethiopia provides the bank with adequate resources and tools to prevent and detect fraud?
- Very well
- Somewhat well
- Not very well
- Not at all well

24. Which of the following statements best describes your experience with the bank's segregation of duties, authorization procedures, and reconciliation processes?
- They are always effectively implemented and prevent most fraud attempts.
- They are generally effective but occasionally require manual intervention.
- They are sometimes inconsistently applied and create vulnerabilities.
- They are rarely followed and significantly increase the risk of fraud.

25. How satisfied are you with the bank's fraud awareness training?
- Very satisfied
- Somewhat satisfied
- Neither satisfied nor dissatisfied
- Somewhat dissatisfied
- Very dissatisfied

26. Please choose the top three options that would most improve the bank's internal control system and its effectiveness in preventing and detecting fraud:
- Enhanced employee training and communication

- Investment in advanced fraud detection technologies
- Strengthening segregation of duties and access control
- Improved reporting procedures and whistleblower protection
- Other (please specify)

27. How would you describe the overall organizational culture at Global Bank Ethiopia? What impact does it have on fraud prevention and detection efforts?

    _____

    _____

    ____

28. How well has the bank adopted new technologies to support internal control activities? What are the challenges and opportunities in this area?

    _____

    _____

    ____