OPERATIONAL RISK IN ETHIOPIAN COMMERCIAL BANKS: A CASE STUDY WITH EMPHASIS ON FINANCIAL FRAUD

BY ZEMICHAEL TESFAMARIAM

Addis Ababa University

College of Business and Economics

Department of Accounting and Finance

A Thesis presented in partial fulfillment of MSc Degree in Corporate Finance with specialty in Investment Management

May, 2025

Addis Ababa, Ethiopia

OPERATIONAL RISK IN ETHIOPIAN COMMERCIAL BANKS: A CASE STUDY WITH EMPHASIS ON FINANCIAL FRAUD

Advisor: Dr. Dakito Alemu (Associate Professor)

A thesis submitted to Addis Ababa University College of Business and Economics, department of Accounting and Finance in partial fulfillment of the requirements for the degree of MSc in Corporate Finance with specialty in Investment Management

June, 2025

Addis Ababa, Ethiopia

Declaration

I, hereby declare that this thesis entitled '**Operational Risk in Ethiopian Commercial Banks: A Case Study with Emphasis on Financial Fraud**', has been carried out by me under the guidance and supervision of Dr. Dakito Alemu. The thesis is original and has not been submitted for the award of any degree or diploma to any institution or university.

Researcher's Name	Signature	Date
Zemichael Tesfamariam Kebte	_____	_____

Certification

This is to certify that the thesis entitles '**Operational Risk in Ethiopian Commercial Banks: A Case Study with Emphasis on Financial Fraud**', submitted to College of Business and Economics, Department of Accounting and Finance for the award of the Degree of Master of Science in Corporate Finance with specialty in Investment Management and is a record of bona fide research work carried out by Zemichael Tesfamariam, under my guidance and supervision. Therefore, I hereby declare that no part of this thesis has been submitted to any other university or institutions for the award of any degree or diploma.

Adviser's Name	Signature	Date
Dr. Dakito Alemu	_____	23/06/2025 _____

Addis Ababa University

College of Business and Economics

Department of Accounting and Finance

Approval of Thesis after Defense

As members of the board of examiners, we examined this thesis entitled '**Operational Risk in Ethiopian Commercial Banks: A Case Study with Emphasis on Financial Fraud**' Zemichael Tesfamariam. We hereby certify that the thesis is accepted for fulfilling the requirements for the award of the degree of 'Masters of Science in Corporate Finance with specialty in Investment Management'.

Board of Examiners

External examiner:

Name	Signature	Date
Dr. Abebaw Kassie		23/06/2025
_____	_____	_____

Internal examiner:

Name	Signature	Date
Dr. Berhanu Beza		
_____	_____	_____

Dedication

To my late father, Liqe Mezemiran Tesfamariam Kebte, for instilling the culture of hard work and determination in me, I know you are in safe hands; and to my mother, Woy. Saba Mulatu as you are my source of inspiration and encouragement. Long live Enaté.
Love you both.

Acknowledgements

A lot of encouragement, assistance and follow-up by my advisor, Associate Professor Dr. Dakito Alemu, has helped me to develop such kind of paper. Thank you for your patience, help, understanding, valuable comments and suggestions.

Lecturers and employees from School of Commerce have helped me a lot in due work and I salute them.

The patience and understanding from my wife, Woy. Belen Tesfaye and our children Oni, Ami, Atnasi and Niye should be appreciated. Love you all abundantly.

Family, colleagues, classmates and friends should be appreciated for their encouragement.

No one can replace the blessing hands of God, for all be in him.

ABSTRACT

This study evaluates the operational risks and financial fraud faced by Ethiopian commercial banks, focusing on internal, human, and external factors that contribute to these issues. It also examines the most prevalent types of fraud and the countermeasures in place. This study employed a mixed-methods research approach to gather data via questionnaires from 236 employees working in 31 commercial banks. A descriptive research design was used to explore and characterize the subject under investigation. Data were sourced exclusively from primary sources, ensuring direct relevance to the research objectives. Ethical considerations were rigorously upheld throughout the data collection process. Additionally, reliability and validity were assessed on a sample basis before analyzing the complete dataset using SPSS. The research identified key internal processes and systems factors that contribute to operational risk. These include inadequate IT systems and infrastructure, weak transaction authentication protocols, a lack of segregation of duties, poor documentation practices, and insufficient real-time monitoring systems. Human factors also played a significant role, such as a weak ethical culture within the organization, a lack of accountability and oversight, a lack of employee training, insufficient background checks during hiring, and employee misconduct. External factors were identified that include cybersecurity threats, political and economic instability, lack of specialized oversight for emerging technologies, weak enforcement of compliance standards, and inconsistent enforcement of anti-fraud regulations. The study documented prevalent types of fraud committed by customers, such as mobile banking fraud, cheque fraud, money laundering, and identity theft, which were identified as the most common. Among employees, the most prevalent types of fraud included debits from dormant accounts, embezzlement, bribery, and collusion with external parties. Additionally, the findings highlighted critical measures for mitigating operational risk and preventing fraud, such as strengthening internal controls, conducting regular audits and monitoring of high-risk accounts, implementing strict access control for sensitive systems, implementing advanced real-time fraud detection systems, and providing regular employee training on fraud prevention. These insights emphasize the importance of a multifaceted approach to mitigate operational risk and prevent financial fraud in the banking sector.

***Keywords**: Ethiopian commercial banks, financial fraud, fraud detection, internal controls, mitigation strategies, operational risk.*

Table of Contents

List of Figures

List of Tables

CHAPTER ONE

INTRODUCTION

1.1. Background of the Study

All over the world, operational risk has become more and more a worry for companies, the myriad of risks ranging from fraud, cybercrime, system failure, to even compliance failure. According to Basel Committee on Banking Supervision (BCBS), it can be understood as a risk of loss arising from insufficient or failed internal processes, systems, people, and external events (BCBS, 2001). More than ever before, increasing complexity in bank operations and new advancements in technology have exposed banks to even more threats. Commercial banks need to manage operating risks so that they can foster financial stability and even more importantly, preserve customers' trust and comply with the regulations (Cristea, 2021).

It is obvious that financial institutions are vital to helping economic growth, but they are becoming more susceptible to the possibility of operational risk with the world being more globalized and technology improving. Identity theft, hacking, and insider fraud are now realities, costing banks billions of dollars annually (Harris, 2024).

In Ethiopia, the National Bank of Ethiopia (NBE) regulates financial institutions, including commercial banks, microfinance institutions, insurance companies, and digital financial service providers, to ensure financial system stability (BBP No. 592/2008). The NBE has implemented policies such as the Financial Consumer Protection Directive (FCP/01/2020) and the Fraud Monitoring Directive (SBB/59/2014) to mitigate fraud risks. However, financial fraud remains a significant threat to commercial banks globally, including Ethiopia (Afjal, et al., 2023).

Over the last ten years, the Ethiopian commercial banking industry has steadily improved along with the market entry of new commercial banks. New opportunities, however, have come with their respective challenges, and one of them is the level of operational risk in the banking system. The weakening of infrastructure and the adoption of newer technologies, along with regulatory restrictions, place Ethiopian banks in very particular risk situations. (NBE, 2024). Operational risk management is a growing area of concern that has not yet been fully researched to understand the scope of its influence in the context of Ethiopian banks. The

purpose of this document is, therefore, to address these considerations by outlining the most salient determinants of operational risk in Ethiopian commercial banks with special emphasis on financial fraud and outlining the proposals for addressing them.

1.2. Statement of the Problem

Operational risk is a major challenge that concerns commercial banks across the world, and Ethiopia is no different. The Ethiopian banking sector has expanded in the past few years. The commercial banks grew from 16 in 2010 to 31 in 2023 (NBE, 2023). However, this growth has fueled fraudulent activities, resulting in significant financial losses and operational challenges. Fraud losses rose by 0.3 billion birr and reached 1.3 billion birr in 2024 (NBE, 2024). One of the most important events in this regard is the March 2024 incident when the Commercial Bank of Ethiopia had a system malfunction that gave clients the ability to withdraw an uncontrolled amount of cash from ATMs and perform fund transfers without limits (Addis Fortune, 2024). This event revealed weaknesses in banking technology and a willingness of people to exploit these gaps. These incidents inflict damages beyond the monetary losses, which include destruction of institutional image and public trust in the banking system (BCBS, 2023).

The Ministry of Justice report further reveals that Ethiopian commercial banks have lost nearly two billion birr to scams, and the bank managers and telecom staff are the ones most likely to be blamed for the acts (Addis Fortune, 2022). The report highlights the seriousness and urgency of the issue by emphasizing the need for an investigation into its causative factors and likely mitigations.

As operational risk management gained more significance, little has been studied about the factors influencing operational risk in Ethiopian banks. There is limited operational risk research in Ethiopian banks. Weak internal controls, inefficiencies in management, and technological weaknesses have been identified as prominent drivers of fraud by local studies (Aragie, 2011; Gebreselassie, 2022; Setarge, 2022). These studies did not fully examine the internal banking and external regulatory gaps that result in operational risk. How these drivers correlate with each other in the context of the Ethiopian banking system has also not been understood. Moreover, a case study by Birhanu tried to reveal that organizational and operational factors, and regulatory loopholes contributed to financial fraud in Ethiopian banks. This study also explained prevalent types of financial fraud along with their preventive

measures. However, the study did not examine the operational risk aspect of the banks in general. In addition, this study could not provide the whole picture of the banking industry as it only studied six commercial banks (one large and five medium banks), ignoring twenty-five small banks which are believed to have had a substantial impact on the result of the study if they could have been added in the study. By acknowledging the above study (Birhanu, 2025), this study tries to bridge this gap by examining the key determinants of operational risk in Ethiopian commercial banks. By identifying these factors, the study aims to provide valuable insights for banks, regulators, and policymakers, enabling them to develop more effective strategies for managing operational risk.

1.3.Research Questions

This study endeavors to tackle the main research question along with its corresponding sub-questions:

1.3.1 Primary Research Question

What are the operational risks in Ethiopian commercial banks**?**

1.3.2 Specific Questions:

- How do internal processes and systems influence operational risk in Ethiopian commercial banks?
- What role do human factors (e.g., employee behavior, training) play in operational risk?
- How do external factors (e.g., regulatory environment, technological infrastructure) impact operational risk?
- What are the prevalent types of financial fraud in Ethiopian commercial banks?
- What strategies can Ethiopian commercial banks adopt to mitigate operational risk?

1.4. Research Objectives

1.4.1. Main Objective

The main objective of this study was to identify the key sources of operational risk in Ethiopian commercial banks.

1.4.2 Specific Objectives

The specific objectives of the study were:

1. To assess the sources of internal processes and systems of operational risk in Ethiopian commercial banks.
2. To evaluate the role of human factors (e.g., employee behavior, training) in operational risk.
3. To analyze the influence of external factors (e.g., regulatory environment, technological infrastructure) on operational risk.
4. To identify the prevalent types of financial fraud.
5. To propose strategies for mitigating operational risk in Ethiopian commercial banks.

1.5. Significance of the Study

This research examines factors that affect operational risk in Ethiopian commercial banks and offers essential insights for various stakeholders:

Policy Contribution: The findings of this study provide valuable insights for regulators and policymakers, enabling them to develop more effective regulatory frameworks for managing operational risk in the Ethiopian banking sector.

Practical Contribution: The study offers practical recommendations for commercial banks, helping them to identify and mitigate operational risks more effectively.

Academic Contribution: By filling a gap in the existing literature, this study contributes to the body of knowledge on operational risk management in developing countries, particularly in the context of Ethiopia.

Future Research Contribution: The findings of this study serve as a foundation for future research on operational risk management in the Ethiopian banking sector and other developing economies.

1.6. Delimitations and Scope of the Study

This study is delimited to Ethiopian commercial banks, excluding other financial sectors (e.g., microfinance, insurance) and non-financial industries affected by operational risk. The focus is justified by data accessibility, sector-specific relevance, and the need for a targeted analysis.

The scope covers five key dimensions of operational risk:

1. Internal factors (processes, systems).
2. Human factors (employee behavior, training).

3. External factors (regulatory environment, technological infrastructure).
4. Prevalent types of financial fraud.
5. Mitigation strategies.

All 31 operational commercial banks in Ethiopia (2024) are included, comprising 1 large bank (CBE), 5 medium banks, and 25 small banks, to ensure representativeness across bank sizes.

1.7. Limitations of the Study

While this study provides valuable insights, the following limitations are acknowledged:

1. Data Constraints: Reliance only on primary data and limited access to confidential bank records may limit the depth of analysis.
2. Context-Specific Findings: Results are primarily applicable to Ethiopia's banking sector and may not generalize to other economies.

1.8. Definition of Terms

To emphasize the key terms addressed in the study, the researcher endeavored to define the issues under consideration both conceptually and operationally.

Conceptual Definitions:

Operational Risk: This refers to the risk of loss resulting from inadequate or failed internal processes, personnel, systems, or external events (BCBS, 2001).

Ethiopia Banking Sector: Banks and financial institutions in Ethiopia provide various financial services, including accepting deposits, granting loans, investing, and making payments (Gashayie & Singh, 2016).

Internal Processes: These are the procedures and systems banks use to conduct their operations, such as transaction processing, risk management, and compliance.

Human Factors: This pertains to the role of employees in operational risk, which includes their behavior, training, and decision-making.

External Factors: These are influences outside the control of the bank that can affect operational risk, such as the regulatory environment and technological infrastructure.

Bribery: This is the act of offering, giving, receiving, or soliciting something of value to influence an individual's actions or decisions in a position of power.

Card Fraud: This involves fraudulent activities using stolen debit or credit cards for unauthorized purchases or cash withdrawals.

Cashier Payment Order Fraud: This refers to the use of counterfeit or manipulated cashier payment orders to defraud individuals or banks.

Cheque Fraud: This includes activities such as forging signatures, altering check amounts, or writing checks without sufficient funds.

Collusion with External Parties: This describes the cooperation between bank employees and external parties to carry out fraudulent activities.

Corruption: This is the abuse of entrusted power for personal gain.

Debit from Deceased Customers' Accounts: This involves the unauthorized withdrawal or transfer of funds from the accounts of deceased individuals.

Debit from Dormant Accounts: This refers to the illegitimate withdrawal or transfer of funds from inactive bank accounts.

Embezzlement: This occurs when employees divert funds or assets for personal use, often by manipulating internal records or creating fake transactions.

Identity Theft: This is when fraudsters use stolen personal information to open accounts or make unauthorized transactions.

Mobile Banking Fraud: This targets mobile banking platforms, gaining unauthorized access through hacking, identity theft, phishing, or manipulation of mobile banking applications.

Money Laundering: This involves concealing the origins of illegally obtained funds through complex transactions.

Opening Fraudulent Accounts: This refers to the act of opening bank accounts using falsified or stolen identities to carry out illegal activities.

Phishing Scams: These are deceptive attempts to acquire sensitive information by posing as a trustworthy entity.

Terrorist Financing: This involves providing, collecting, or managing funds intended to support terrorist activities.

Transaction Reversal Fraud: This is the deliberate manipulation of accounts by reversing legitimate transactions.

1.9. Organization of the Study:

The first chapter of the study serves as an introduction, covering the background of the study, the statement of the problem, research questions, objectives, and other relevant matters. The next chapter consists of a comprehensive review of literature directly related to the topic, presenting both theoretical and empirical evidence from around the world along with a conceptual framework to enhance understanding. The subsequent chapter discusses the research methods employed, detailing data collection, sample selection, sampling techniques, and research design. Chapter four focuses on presenting and analyzing the outcomes, highlighting key findings through data analysis and interpretation. Finally, chapter five summarizes the key points discussed earlier and offers recommendations based on the research findings.

CHAPTER TWO

LITERATURE REVIEW

Introduction

This chapter assesses both theoretical and empirical literature regarding operational risk, with an emphasis on fraud as a significant element. Additionally, the review investigates the banking sector in Ethiopia, pointing out shortcomings in regulation, vulnerabilities in information technology, and trends related to fraud. Research findings indicate that ineffective internal controls and human elements are significant risks. The chapter wraps up by highlighting areas needing further research and suggesting a conceptual framework that connects operational risk, fraud, and strategies for mitigation.

2.1. Theoretical Literature Review

2.1.1 Definition and Scope of Operational Risk

Operational risk refers to a generic term that encompasses risks inherent from internal or external sources in the processes of technology, human interaction, and external factors. Basel II and III frameworks provide a structured approach for the identification, assessment, and monitoring of operational risk (BCBS, 2011). The three basic components of operational risk, according to Basel, are:

- ✓ Process and system Risk: Process failures in a bank, such as errors in transactions, settlement failure, documentation failure, and poorly designed processes. The risks here primarily stem from inefficient processes or a lack of standardization. When we come to system risk, disruptions to IT systems, software, and hardware that hinder bank operations.
- ✓ People Risk: Risks due to human error, improper employee training, poor behavior, and excessive employee turnover. People risk is most evident in banks with large numbers of employees and complex operational structures.
- ✓ External Event Risk: Risks resulting from events that are external in origin such as natural disasters, political unrest, regulatory changes, and economic disruptions. These are usually outside the control of the bank but can be highly operationally significant.

2.1.2 Theoretical Models of Operational Risk

There has been the development of several theoretical models used to understand and regulate operational risk. These models provide frameworks for the measurement and mitigation of operational risk:

- Loss Distribution Approach (LDA): A Statistical method used to quantify the frequency and severity of operational risk events. LDA is based on using historical data to estimate potential losses and is widely used in risk management (Cruz, 2002).
- Scenario Analysis: A qualitative method that uses hypothetical scenarios to assess possible operational risks. This method is especially useful in analyzing low-probability, high-impact events (BCBS, 2011).
- Key Risk Indicators (KRIs): Metrics used to track and predict the occurrence of operational risk events using historical data and trends. KRIs are precursors to risks (Chapelle, et al., 2008).
- Control Self-Assessment (CSA): A procedure where business units assess their own controls and risks. CSA helps identify gaps in risk management procedures (Power, 2007).

2.1.3 Operational Risk Management Frameworks

According to various studies and reports, for successful operational risk management, there should be a solid framework, which includes the following elements:

- Risk Identification: The identification of potential causes of operational risk in the bank. It encompasses defining all business processes and identifying vulnerabilities (Lam, 2014).
- Risk Assessment: In this step, the likelihood and potential impact of the identified risks are both estimated. It makes use of quantitative techniques such as risk scoring as well as qualitative techniques such as expert opinion (Hopkin, 2018).
- Risk Mitigation: This is putting controls and procedures in place intended to reduce the likelihood and impact of operational risks. This may include process improvement, employee training, and the acquisition of technological facilities (Fraser & Simkins, 2016).

- Risk Monitoring and Reporting: This involves ongoing observation of operational risks and reporting them to senior management and regulators. This helps ensure that the risks are addressed proactively and are in keeping with regulatory requirements (BCBS, 2011).

Among the various forms of operational risk, fraud has emerged as an increasing and ongoing risk to commercial bank profitability and stability. Fraud is selected as the subject of this literature review because it is a significant component of operational risk; and its causes, impacts, and control measures are addressed in this overview. Consequently, the focus of this research will primarily revolve around operational risk and, thereby financial fraud.

2.1.4 Definition of Fraud:

Fraud has been defined by the International Auditing and Assurance Standards Board (IAASB) as a deliberate act performed knowingly by one or more individuals from management, individuals charged with governance, employees, or third parties that entails the use of deception to obtain an illegal or unfair advantage (IAASB, 2022). Association of Certified Fraud Examiners (ACFE) defines fraud as any act relying on deceit for its accomplishment, and it is a crime when it constitutes a willful distortion of fact or concealment of a material fact to induce one to act at his or her detriment (ACFE, 2023). National Bank of Ethiopia (SBB/59/2014) states that fraud is an act or omission by shareholders, directors, employees, and customers made with the intent to gain dishonest or illegal advantage for the fraud perpetrator or for some other party. Digital fraud, according to the Basel Committee, is fraud carried out by third parties through electronic means such as mail, websites, and malware that aims at stealing bank property or passwords of bank customers. Digital fraud lies on the inability of a bank or its clients to properly distinguish between a counterfeiter and a legitimate counterparty. The operations are targeting account management systems, card processing systems, and banking applications. Fraud can be categorized in many ways, and each category has individual or organizational characteristics (BCBS, 2023).

Fraud against individuals by targeting individuals by fraudsters through a method of identity theft, phishing frauds, and any other method. Fraud against organizations can be viewed from two viewpoints: internal organizational fraud and external organizational fraud. Internal organizational fraud (occupational fraud) where an employee, manager or senior executive of an organization defrauds himself/herself by embezzlement, tax evasion, and making false

statements to investors and stockholders. External organizational fraud is fraud committed against an organization by its customers and hackers (ACFE, 2024). Elliot & Willingham characterize fraud as management fraud and employee fraud. Most common frauds committed by managements include financial statement fraud, material fact misrepresentation misappropriation of assets, material fact concealment, illegal transactions, bribery, corruption, and conflict of interest (Elliott & Willingham, 1980). Most common frauds committed by employees other than managements include embezzlement, breach of fiduciary duty, and misappropriation of trade secrets or intellectual properties. The customer fraud is the fraud committed by the customers for undue benefit. Most of the crimes committed by the customers in the bank are identity theft, pinching another customer's password for card or mobile banking and cashing out illicit money, handing over counterfeit notes to the counter, etc. (Setarge, 2022). Silverstone & Davia categorize fraud into three types: fraud exposed and known publicly, fraud discovered by an organization but not disclosed, and fraud that has not been detected. The present study emphasizes causes of frauds exposed and known publicly as well as frauds discovered by an organization but not disclosed (Silverstone & Davia, 2005). Zahra with her colleagues classify fraud offenders as active participants and passive acquiescence based on the extent to commit the fraud. Active participants are the person who actively participated in the fraud activities, whereas passive acquiescence are typically supervisors or managers who are aware of illegality in the firm but are unwilling to take any corrective measures (Zahra, et al., 2007).

2.1.5 Theories of Fraud

Various scholars named several theories concerning fraud, the most famous and known of which is fraud triangle theory studied by Cressey D. in his early work of 1973 (Cressey, 1973). Another similar theory named by Setarge are differential association theory, job dissatisfaction theory, fraud scale theory, and fraud diamond theory (Setarge, 2022).

2.1.5.1 Fraud Triangle Theory

The Fraud Triangle Theory, which was created by criminologist Donald Cressey, is one of the most popular fraud models. He studied embezzlers who were incarcerated in various jails across the Midwest US. He, then, concluded that "trusting individuals turn into trust violators when they come to believe that they possess a non-shareable financial problem, become aware that this difficulty can be covertly addressed by violating their role of financial trust, and justify

their behavior in a way that allows them to reconcile their self-concept as a trusted individual with their behavior." The Fraud Triangle has three components: pressure, opportunity, and rationalization, each of which is a distinct aspect of the motivations of the individual to engage in fraud. Pressure involves economic or affective burdens experienced as "non-shareable." Cressey outlines six non-shareable problems, which include non-fulfillment of responsibilities, failure as an individual, losses in business, solitude, status-grabbing pressures, and problems in employment. He emphasized that what is "non-shareable" varies among individuals; what is bearable to one person may be intolerable to another, hence fraudulence (Cressey, 1973).

Opportunity is the second pillar of the triangle. For fraud to take place, people do not only need to be under pressure but also believe that they can get away with committing fraud (Akers & Gissel, 2006). Cressey discovered that most of them at first do not take advantage of these opportunities but come to see their fiduciary status as providing a means to solve their dilemmas. Rationalization is the psychological process by which the perpetrator rationalizes their behavior. This is not an after-the-crime explanation, but rather more of an integral part of their motivation. According to him, fraudsters use verbalization common for their environment or culture so that they are able to align their behavior with their self-concept of people (Cressey, 1973).

2.1.5.2 Theory of Differential Association

The Theory of Differential Association was presented by Edwin Sutherland, a famous white-collar crime researcher, in the 1930s. He coined white-collar crime for crimes committed by a businessperson against shareholders or the public (Sutherland, 1949). In his theory, criminality is learned and develops through the process of social interaction where exposure to favorable attitudes towards crime results in deviance.

The learning process involves both techniques of committing crime and the motivations and justifications that maintain criminality. Opportunity Pressure Rationalization. He argues that exposure to conflicting social values influences criminality; individuals are more likely to be criminal when they are exposed to more pro-criminal values than anti-criminal values. Critics of the theory, like Akers, argue that Sutherland's theory cannot explain all types of deviance or crimes that do not seem to involve learned behavior (Akers, 1996).

2.1.5.3 Job Satisfaction Theory

Hollinger & Clark studied 12,000 employees and found that job dissatisfaction was a main motivator of employees' fraud. Employees who felt their work or jobs were unfair were more inclined to rationalize and engage in fraud (Hollinger & Clark, 1983). Nevertheless, since there is a lack of general information on employee theft, the theory is difficult to generalize, and it shares motivational and rational limitations with the Fraud Triangle Theory (Wells, 2013).

2.1.5.4 Fraud Scale Theory

Albrecht and his colleagues developed the fraud scale, an extension of Cressey's model with one additional element: personal integrity. The fraud scale theory contends that fraud results from a convergence of situational pressure, perceived opportunities, and low personal integrity. Fraud, in the view of Albrecht, will more likely take place with high situational pressures and opportunities, and low personal integrity. The inclusion of personal integrity is a significant enhancement to the fraud triangle since it offers more explanation as to why people perpetrate fraud (Albrecht, et al., 1984).

2.1.5.5 Fraud Diamond Theory

Wolfe & Hermanson expand on Cressey's Fraud Triangle by introducing a fourth element, capability- hence the Fraud Diamond. They argued that, in addition to pressure, opportunity, and rationalization, the perpetrator must possess the technical skill, confidence, and competence to execute the fraud. Cognitive skills, including biases and social manipulation, also perform an essential function in determining whether one is able and willing to commit and conceal fraudulent activities (Wolfe & Hermanson, 2004). In another study, this theory was also discussed as the involvement of co-conspirators, who may unconsciously assist in the fraud due to social manipulation, a concept referred to as social engineering (Omar & Din, 2010).

2.1.6 Types of Fraud

Fraud in banking institutions is categorized into internal and external fraud. Both are highly dangerous for financial institutions, impacting financial stability and reputation. Internal fraud is committed by individuals within the bank, including employees and others who have privileged access to bank resources (BCBS, 2021). Greenbaum & Thakor refer to insider fraud as a significant problem, typically facilitated by weak control systems (Greenbaum & Thakor, 2007). The Association of Certified Fraud Examiners (ACFE) reported sizable global activity

in 2020, with 2504 cases tallying $ 3.6 billion in losses (ACFE, 2020). Embezzlement, insider trading, self-dealing, and falsification of records are a few of the common forms of internal fraud (Zahra, et al., 2007). External fraud originates from outside the bank. Wendels and his colleagues claimed that they grouped external fraud into two general categories. New account fraud is when a false identity, stolen or fabricated, is utilized to open an account, and the account is then utilized to obtain loans or credit under deceptive pretenses. Existing account fraud is when an existing account is tapped for unauthorized use, typically accomplished through phishing, hacking, or other cyber-attack techniques. Existing account fraud is more easily detected, as algorithms readily identify suspicious account behavior (Wendels, et al., 2009). Third-party individuals, such as customers or business partners, who induce bank staff to commit fraud through bribery or kickbacks may also comprise external fraud (Mishkin, 2006).

2.1.6.1 Unauthorized Withdrawals

Unauthorized transactions are marked by the withdrawal or transfer of money from a bank account by someone other than the account owner and without the owner's approval. Yalew (2021) explains that such transactions are usually a consequence of divulging sensitive information like social security numbers or account details. Withdrawal fraud can be undertaken through forgery like counterfeiting a customer's signature or transferring money without any mandate, most frequently for savings, deposits, or current accounts (Yalew, 2021).

2.1.6.2 Unauthorized Use of Credit or Debit Cards

Credit Card fraud is prevalent too, characterized by unauthorized usage, card cloning, and phishing attacks. Joshi states that with increasing online transactions, the possibilities for fraudsters to breach credit card information also increase. This not only inflicts monetary losses for banks but exposes customers to threats too, demanding enhanced security solutions and customer awareness (Joshi, 2022). Fraud via unauthorized credit or debit card transactions is the charging of purchases or other expenses without the cardholder's permission. The unauthorized use of a card can be caused by lost, stolen, or counterfeit cards, or fraudulently issued cards (Yalew, 2021).

2.1.6.3 Theft and Embezzlement

Theft and embezzlement are also forms of insider fraud, which involve the unlawful acquisition of cash, checks, or other financial instruments from the bank. Chelangat identifies

embezzlement as a prevalent practice, particularly in organizations where financial controls may be lacking (Chelangat, 2014).

2.1.6.4 Account Opening Fraud

Account opening fraud is perpetrated when an individual opens a new bank account using fictitious details or false identification. Onkagba chronicles that this kind of fraud is generally found out in the first ninety days of account operation, typically when counterfeit cheques are deposited and withdrawn a short time later, thereby leaving the bank at financial loss (Onkagba, 1993).

2.1.6.5 Computer Fraud

Technological innovation has increased computer fraud, which involves the use of electronic systems to steal or manipulate information. Computer fraud targets banks' security systems either through hacking or accessing accounts of customers without any authorization (Onkagba, 1993).

Fraudsters do this either to demonstrate their technical capability or to gain financially. The rise of cybercrime associated with internet banking is also a significant problem. Phishing, malware, and social engineering are used by cybercriminals to exploit customer credentials. The compromised credentials can be employed to execute unauthorized transfers from customer accounts, emphasizing the requirement for rigorous cyber security controls (Joshi, 2022).

2.1.6.6 Money Laundering

Money laundering refers to the act of concealing the origin of illegally obtained money, typically by passing it through a complex chain of bank transactions or commercial deals (Chen, 2024). It is typically associated with terrorism financing, organized crime, and drug trafficking, where illicit money is converted to appear legitimate through the use of financial institutions.

2.1.6.7 Identity Theft

Joshi cites a number of banking fraud types that significantly impact financial institutions. Among the significant issues cited is identity theft, where fraudsters take advantage of weaknesses in identity authentication systems to gain unauthorized access to customer accounts. This often involves unauthorized use of sensitive personal information like

Permanent Account Number (PAN), which requires banks to make their authentication systems stronger to guard against this kind of weakness (Joshi, 2022).

2.1.6.8 Loan Fraud

Loan application fraud is another issue. Internal and external stakeholders, in most cases, engage in fraudulent activities, such as document forgery, overestimation of collateral, and diversion of funds for some projects. These lead to enormous financial losses for banks and undermine the overall integrity of the lending process. Implementing more stringent verification processes and audits is necessary to avoid these risks (Joshi, 2022). Josh's work centers on the risk of insider fraud being perpetrated by bank employees. These are people who have the ability to utilize their positions to steal, manipulate data, or enable attempts at external fraud. This insider threat is double-edged: not only does it directly result in financial loss but it also incapacitates the reputation of the banking organization. To offset this, the banks must have a good internal control, regular audits, and a moral work environment.

2.1.7 Reasons that Lead to Commit Fraud

Human beings are subject to another pressure of fraud not the junior staff but also the top managements. Three key sets of factors- societal, industry, and company level are there to be a factor which can influence employees as stated by Zahra and her colleagues. Individuals who are unable to meet their goals in conventional means experience tensions, and may want to discharge this tension by using unwanted or abnormal means in order to achieve their goals. Employee's past could be a crucial element to decide his or her wish to commit fraud. Out of the most suitable variables age, experience, education, gender, and ability of self-control all are a serious consideration (Zahra, et al., 2007). Age the younger the more the more willing to commit fraud and risk-taking activities, the employee with shorter tenure in the position the more likely to commit illegal activities, the education level is positively related with the moral development results to abstain and avoid such wrongdoing activities, females are less involved than males in such mal-activities, individuals with low self-control trait are likely to commit frauds. The rapid application of internet products in banking services to make its application easier, has also introduced new avenues for fraud exploitations on the part of cybercriminals exploiting technology vulnerabilities to launch an attack on computer systems. Absence of regulatory provisions also plays an important role in facilitating fraud.

If regulations fail to keep pace with evolving banking activities and digitalization, fraudulent process tends to go unnoticed or unmonitored. Joshi calls for stricter and stronger regulations, along with effective enforcement mechanisms, to curb this issue and create a stronger banking system. Another Contributing factor is the lack of cyber security awareness among customers and bank employees. Lack of information regarding cyber security best practices puts both groups at risk of phishing, social engineering, and other cyber attacks (Joshi, 2022). Internal collusion and corruption within banks also enhance the risk of fraud. Employees engaged in corrupt practices or collude with external fraudsters present opportunities for financial exploitation that are difficult to discover and rectify.

2.1.8 Preventive Measures and Detecting Mechanisms

Fraud prevention relies on developing an ethical workplace culture and possessing effective internal controls. Leadership needs to set the example for ethical behavior and communicate clearly that fraud will not be tolerated at any level.

Effective controls prevent fraud through tough processes for vetting customers, vendors, and business partners. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has an extensive framework available for building these controls. Training is necessary to prevent, as employees must understand that they have a critical role in the prevention of fraud. Successful fraud training includes new employee orientation, concentrated training on jobs with high risk, regular refresher training, and post-training assessments. Institute of Internal Auditors (IIA) also focuses on detective controls to detect fraud where it occurs, as a complement to preventive methods such as whistleblower hotlines and feedback mechanisms anonymous reporting mechanisms, such as hotline web forms, and exit interview (obtaining information from departing employees), encourage employees and stakeholders to report unethical behavior or fraud occurrences, surprise audit and real-time monitoring of risky sites can detect fraud before its large-scale occurrence. Technology has a dual role to fulfill in the fight against financial fraud in commercial banks (IIA, 2009). While it provides fraudsters with new means of committing fraud, it also assists banks in detecting and fighting fraud more effectively. Emerging technologies such as data analytics offer effective tools to discover fraud patterns and anomalies (Quah & Sriganesh, 2008). Fraud detection technology and data analytics software allow banks to move from reactive to proactive, real-time fraud detection, significantly reducing potential financial losses (Mueller, 2015).

New technologies like biometric authentication, device fingerprinting, behavioral analytics, and out-of-band authentication have also enhanced security in online banking. All these notwithstanding, no solution can eliminate fraud entirely. An all-layered approach utilizing these tools is required to remain ahead of continuously evolving fraud schemes (Geffner, 2014). Technology will not secure in isolation, yet when paired with effective policies and trained employees, it delivers immense protection and advance warning against evolved fraud schemes (Mueller, 2015). While technology has made more advanced types of fraud possible, it also presents robust prevention and detection measures. Sophisticated techniques, including social network analysis, dynamic account modeling, and forensic accounting, can detect abnormal patterns and reduce fraud threats. Banks, however, need to continually update their systems to remain one step ahead of new fraud mechanisms. Successful fraud prevention demands cooperation between banks and their customers. Banks need to inform customers about fraud threats and liabilities and implement strong cybersecurity protocols. Organizations have also to adopt an open perspective, offer fraud patterns and methods, and offer legal action by efficient evidence collection (Bhasin, 2016).

2.1.9 The Ethiopian Banking Sector

Ethiopia's banking system, the largest part of financial intermediation, has a major impact on the country's economic structure. It plays a key role in growing and developing the nation's economy. Ethiopia sits in Africa's northeast region and ranks among the continent's ten biggest countries. The public sector leads its economy, making it one of the world's most closed systems. Yet, Ethiopia's banks are both interesting and troublesome (ACFE, 2024). As of the end of June 2023, Ethiopia had 31 banks, all of which were domestic. Among these, the Development Bank of Ethiopia (DBE), a development finance institution, held nearly five percent of the sector's total assets. The remainder included three full-fledged interest-free banks, five microfinance institutions that had transitioned to commercial banks, and 22 conventional commercial banks, including the largest, the Commercial Bank of Ethiopia (CBE). Except for DBE and CBE, all other banks were private (NBE, 2024).

2.1.10 Ethiopian Banking Sector's Role in the Economy

The banking sector plays a crucial role in the Ethiopian economy. As of the end of June 2023, total deposits reached Birr 2.2 trillion, representing 24.8 percent of GDP, while total loans and bonds amounted to Birr 1.9 trillion, or 21.7 percent of GDP. Deposits increased by 24.6

percent, driven by significant growth in both savings and time deposits, and loans and bonds grew by 24.3 percent. However, GDP grew at a faster pace. Consequently, the share of deposits in GDP decreased from 28.2 percent the previous year to 24.8 percent, and the share of loans and bonds fell from 16.0 percent to 14.3 percent. Compared to international standards, the share of loans in GDP remains low, intending to substantially increase it in the medium term to mitigate credit concentration risk (NBE, 2024). However, it is important and wise to acknowledge and appreciate the strengths and advantages of the Ethiopian banking sector. As we look towards the future with optimism, both the internal dynamics of the banking sector and external economic influences will undoubtedly have an impact on its core operations. The ability of banks to adapt to advancements will play a crucial role in their ongoing success within the changing FinTech landscape (Addis Fortune, 2024). Furthermore, the National Bank of Ethiopia (NBE) classifies commercial banks into three categories based on their asset size: large, medium, and small banks (see Table 2.1). Their roles in the market are outlined as follows:

Large Bank: The only large bank in the country is the state-owned CBE. Although its market share declined from the previous year, CBE still remains a systemically important bank. At the end of June 2024, its total assets and deposits constituted just under half (47.9 percent and 47.1 percent, respectively) of the whole banking sector. However, its total capital accounted for just less than a quarter (24.2 percent) of the total.

Medium Banks: The combined share of the five medium-sized banks 10 in the industry increased for all key balance sheet items in the year to the end of June 2024 compared to a year earlier: combined assets went from 28.0 percent to 28.9 percent of the sector's total assets, total deposits from 29.4 percent to 30.3 percent of the sector's total, and capital from 31.0 percent to 33.0 percent. Nevertheless, despite the growing market share, no medium-sized bank is currently regarded as a systemically important bank.

Small Banks: At the end of June 2024, the combined assets and deposits of the 25 small banks 11 accounted for 23.3 percent and 22.7 percent, respectively, of the whole banking sector – an annual increase of 0.8 percentage points each. Likewise, their combined total capital share increased from 41.6 percent of the sector's total capital in 2023 to 42.8 percent at the end of June 2024. The growth of the small banks' aggregate market share can be explained by their

increasing number over the years and the rapid initial expansion of the newly established banks. However, with an individual share in assets, deposits, loans, and bonds of less than two percent, none of the small banks can be considered systemically important.

Table 2.1: Type of Banks in Ethiopia by Size & Ownership

Type of Bank	Total Assets		Total Loans & Bonds		Total Deposits		Total Capital	
By Size Class	June 2023	June 2024	June 2023	June 2024	June 2023	June 2024	June 2023	June 2024
Large	49.5	47.9	46.7	45.2	48.7	47.1	27.5	24.2
Medium	28.0	28.9	30.5	31.1	29.4	30.3	31.0	33.0
Small	22.5	23.3	22.9	23.7	21.9	22.7	41.6	42.8
By Ownership	June 2023	June 2024	June 2023	June 2024	June 2023	June 2024	June 2023	June 2024
Public	49.5	47.8	46.7	45.2	48.7	47.1	27.5	24.2
Private	50.5	52.2	53.4	54.8	51.3	52.9	72.6	75.8

Source: NBE Database and Off-site Reports

Category of Banks:

1. Large Bank: Commercial Bank of Ethiopia
2. Medium Bank: Awash Bank, Bank of Abyssinia, Cooperative Bank of Oromia, Dashen Bank, Hibret Bank.
3. Small Bank: Abay Bank, Addis International Bank, Ahadu Bank, Amhara Bank, Berhan Bank, Bunna Bank, Enat Bank, Gadaa Bank, Global Bank, Goh Betoch Bank, Hijra Bank, Lion International Bank, Nib International Bank, Omo Bank, Oromia Bank, Rammis Bank,

Shabelle Bank, Sidama Bank, Siinqee Bank, Siket Bank, Tsedey Bank, Tsehay Bank, Wegagen Bank, ZamZam Bank, Zemen Bank.

2.2 Empirical Literature Review

2.2.1 Global Perspectives on Operational Risk

The empirical literature on operational risk in commercial banks has identified some key factors leading to operational risk. These are:

- Lack of Strong Internal Controls: There has been a very evident source of operational risk, which is a weakness in internal controls. Research shows that banks with strong internal control mechanisms have the competency to manage operational risks (Hoffman, 2002). The occurrence of operational failures is reduced in the case of banks which employ automated controls and very frequent audits.
- Human Error: Human error, which involves mistakes committed by employees in normal operations, has been identified as one of the most significant sources of operational risk. It is believed that training and development can reduce this type of risk (Chernobai, 2007). For instance, banks that focus on employee training record fewer errors in transactions.
- System Failures: IT system failures, such as software bugs and hardware failures, have been identified as a significant source of operational risk. The banks are at better position in managing this risk if they invest in robust IT infrastructure (Allen & Bali, 2007). For instance, banks with extra systems and disaster recovery plans have minimum downtime.
- External Events: External events, like natural disasters and political unrest, have been found to impact operational risk extensively. Banks that have plans in place, as quoted by Alexander, are better able to withstand the impact of such events. Banks with business continuity plans, for instance, are able to restore operations with ease after an interruption (Alexander, 2003).

2.2.2 Operational Risk in African Commercial Banks

In the African context, operational risk has been a significant concern for commercial banks. Studies have shown that:

- Regulatory Environment: The regulatory environment in many African countries, including Ethiopia, is often underdeveloped, leading to higher operational risks. Banks that operate in countries with strong regulatory frameworks are better able to manage

operational risks (Adekunle & Adetiloye, 2013). For instance, compared to other banks in other nations of Africa, South African banks, whose regulatory environment is developed, have less operational risk.

- Infrastructure Issues: Unreliable power supply and poor IT systems are just some of the substandard infrastructure discovered to be one of the major sources of risk in African banking operations. Those banks that invest in building infrastructure are better positioned to manage this risk, state Owojori and his colleagues. Banks that use generators as backups and cloud computing systems face less interruption (Owojori, et al., 2011).
- Human Resource Management: Lack of proper training and development has been identified as one of the key causes of operational risk within African banks. Banks are in a better position to control such a risk when they invest in staff training and development (Adeyemi, 2011). Such banks that routinely train employees to deal with newer systems and methods commit fewer errors.
- External Events: External events such as natural disasters and political instability have been found to have a significant impact on operational risk. Banks that have contingency plans in place are better able to manage the impact of these events (Alexander, 2003). For instance, banks with business continuity plans can resume operations quickly after a disruption.

2.2.3 Ethiopian Commercial Banks' Operational Risk

Ethiopian commercial banks are more and more focused on operational risk. Empirical studies have also pointed out some key factors influencing operational risk in Ethiopian banks:

The regulatory framework in Ethiopia is evolving, and banks generally face challenges in adapting to new regulations. In the opinion of Abebe, banks with well-functioning compliance departments are in a better position to manage operational risks. For instance, when banks hire compliance officers and carry out frequent compliance checks, they report less regulatory fines (Abebe, 2015).

- IT Infrastructure: Inadequate IT infrastructure is a common problem in Ethiopian banks, increasing operating risks. Tadesse clarifies that banks can better deal with this risk when they make investments in IT infrastructure. Banks utilizing cybersecurity

and next-generation core banking systems, for instance, experience fewer system failures (Tadesse, 2016).

- Human Resource Management: Lack of employee training and development has been one of the major causes of operational risk in Ethiopian banks. Banks are in the best position to deal with this risk when they put money into training and employee development (Gebremichael, 2017). Banks that train employees on new processes and technology, for instance, see improved staff performance.
- Process Management: Poor internal processes, such as transactional errors and settlement breakdowns, have been cited as one of the main drivers of operational risk in Ethiopian banks. Effective internal procedures help banks better control this risk. Banks that use regular process checks and standardized procedures, for example, make fewer errors (Mulugeta, 2018).

As stated earlier, since fraud is a significant component of operational risk, the next part of the study will incorporate empirical evidence around the globe in general and Ethiopia in specific.

2.2.4 Global Perspectives on Fraud

Bank fraud is a universal problem worldwide, as is seen in studies that have reviewed internal and external fraud sources, such as employees, customers, and third-party suppliers. Banks, due to their liquidity levels and huge financial assets, are particularly vulnerable to fraud operations such as money laundering, loan fraud, and asset misappropriation. Sanusi and his colleagues (2015) in Malaysia carried out a study on common forms of fraud in the banking sector. Money laundering (46%) and loan fraud (29%) were most common in mortgage loans, while loan fraud was most common in hire purchase loans (69%). The study also indicated that remittance frauds typically involve tampered US Treasury Cheques, with substantial losses, as fraudsters exploit the knowledge of the clearing system to escape detection. Exchange of notes fraud and ATM fraud are also common, with sophisticated methods used to deceive bank staff and customers. Cheque manipulation by fraudsters involves removal of payee name through chemical treatment or scraping, with tampered cheques being cashed to avoid detection. This placed the need for strong internal controls and verification measures in the spotlight. Housing loan frauds include fake documents and overvalued properties, which are usually facilitated by

bank personnel. Adherence to strict verification procedures and the employment of sound valuers is required to prevent these risks (Sanusi, et al., 2015).

2.2.5 Ethiopian Commercial Banks' Fraud

Worku explained that there was a strong relation between the functionality of internal control systems and reducing fraud in Ethiopian banks. In particular, every aspect of internal control systems expresses high influence against fraud prevention and detection, particularly with monitoring processes and risk measurement being highly effective. From the conclusion, the overall internal controls in Ethiopian banks are found to be good in general; yet there are places that are necessary to enhance strengthening the controls even further (Worku, 2018).

Worku examined the causes and nature of e-banking fraud in Ethiopian banks, evaluating the effectiveness of fraud management practices and potential areas for improvement. Based on semi-structures interview and document analysis from three banks, the research provided an overview of prevalent e-banking fraud types, including card skimming and phishing, and addresses factors such as technology gaps and skill shortages that contribute to fraud vulnerabilities (Worku, 2020).

Getachew examined the impact of internal control systems on fraud prevention in the Ethiopian Commercial Bank. The study confirmed that each element of internal controls-control environment, risk assessment, control activities, information and communication, and monitoring prevents fraud in a meaningful way. Each element has a positive impact on fraud risk reduction. The study found that successful internal controls have an important function in preventing fraud and that all components of the control contribute to reducing fraud in the Ethiopian banking industry (Getachew, 2021). Gebreselasie investigated common bank frauds, their reasons, and the effectiveness of fraud avoidance and detection systems in Ethiopian banks. This study highlighted the application of internal controls, training, and forensic accounting in addressing fraud risk, identifying areas of deficiency in existing procedures and advising on improving fraud management. General frauds which are shown are cash thefts, cheque forgeries, fraudulent documents, and internet banking fraud. The employees or customers primarily commit these frauds at times with involvement from third parties. Critical control factors that lead to fraud are complacency, transparency, and poor management controls. Various methods of fraud prevention and detection are employed by banks, including

data mining, employee background checks, random audits, IT controls. The practice of job rotation does not exist, and employees involved in fraud remain in their jobs without anyone noticing (Gebreselasie, 2022). Aragie established that fraud prevalence among Ethiopian banks can largely be accredited to inadequate internal controls, managerial policy, and lack of effective employee monitoring. Additionally, low compensation, few job rotations, and limited monitoring of employees are also avenues of opportunity for fraud (Aragie, 2011). The study raised the evidence that both repetitive small-value frauds and big-value frauds are risk-generating sources among banks, impeding trust as well as economic stability. The type of frauds observed includes frauds being performed directly against the bank or its customers and frauds by managers or employees. Also, the research found collusion with outsiders by bank staff and even fraud by outsiders, e.g., robbers.

Bhasin indicated that fraud should be combated in the Indian banking sector through an active and multi-dimensional approach. Banks can enhance the safety of transactions using cryptographic screening, staff rotation in vulnerable positions, alertness, technological upgrade, and involving more individuals in high-value transactions. The study further highlighted the internal auditors' role with an important contribution coming through technical capability, learning, and judicious management practices by mastering advanced technology-driven tools (Bhasin, 2015). As the use of ICT is on the rise, fraudulent activities are more complex, and more information needs to be exchanged between financial institutions and they need to embrace data mining techniques for detecting insider fraud. Training and development of fraud awareness among employees were also found by the study to be a necessary tool. Bhasin also stated that fraud prevention in banking is multi-dimensional. While banks can't achieve a zero-fraud scenario, proactive steps such as risk evaluations, utilizing newer technologies like data analytics, neural networks, and encryption, and enhancing internal governance are essential. Some of the main recommendations include simplifying reporting systems, addressing staff accountability, and improving fraud risk management practices under senior leadership oversight. Higher incidence of internet banking fraud, ATM card fraud, and impersonation fraud highlights the importance of customer awareness, education, and participation in combating fraud. The study continued to profile forensic accounting as a major capability in effective fraud investigation, including the collection and analysis of evidence to support court cases. He maintains that it is not possible to create a zero-fraud culture but adds

that banks can drastically reduce fraud threats through proactive policies, technology, and cooperation with the government (Bhasin, 2016).

Dennis and his colleagues conducted determinants of employee fraud in the banking sector in Ghana with the focus on implications of corporate culture, internal controls, and some aspects of fraud drivers. It reaffirmed that capability, opportunity, rationalization, and pressure are key driers of employee fraud in Ghanaian banks. The study confirmed that the internal control weaknesses created opportunity for fraud and that managerial as well as non-managerial employees were engaged in fraudulent activities. Types of fraud committed by the employees included kickbacks, misstatement of expenses, property misappropriation, and thefts of cash that depict the complicated factors involved in employee fraud (Dennis, et al., 2018).

Setarge also enumerated the most common fraud types in Ethiopian banks, namely money transfer fraud, unauthorized withdrawal, theft and embezzlement, account opening fraud, money laundering, document manipulation, and ATM fraud. Managerial fraud of various forms, including overstatement of revenues and overvaluation of assets, was also mentioned in the study. Socio-cultural forces (e.g., crime rates, ethics, and education), economic pressure, poor training, and rising technology sophistication, in line with the Fraud Triangle Theory's opportunity, rationalization, and pressure model of major fraud drivers, are fraud causes (Setarge, 2022).

Wanjohi identified poor internal control and accounting systems as the foremost drivers of fraud in the Commercial Bank of Africa (CBA). Challenges such as lack of supervision, inadequate customer due diligence, and inadequate staff policies were primary contributing factors to fraud. CBA fraud was broadly categorized into employee fraud, which was the most common and includes forgery, asset misappropriation, and unauthorized account alterations; third-party fraud, wherein there was employees' collusion with outsiders in matters such as cheque fraud; and management fraud, typically consisting of manipulation of the financial reporting. The study also emphasized the importance of ICT tools such as firewalls and password, rigorous audits, and encouraging an ethical work environment as effective fraud prevention practice (Wanjohi, 2014).

2.3 Literature Gap

In Ethiopia, even though operational risk remains a critical threat to society, banks, and the country at large, fewer than insufficient research has been conducted on the subject. In the past few years, the issue has been on the rise and must be researched to find the causes and the preventive actions. In most research, the causes of fraud have not been investigated thoroughly, and the organizational and operational causes have not been investigated thoroughly. Being aware of this gap, the researcher aimed to conduct a study of determining factors affecting the operational risk of commercial banks in Ethiopia. This study provides an in-depth explanation of operational risk in general and financial fraud in particular, and it presents a necessary knowledge base for developing effective preventive strategies.

2.4 Conceptual Framework

[Operational Risk] → [Financial Fraud] → [Mitigation Strategies]

This conceptual framework is designed based on the following scholarly works and reports. The BCBS highlights in its 2011 report that weak internal controls, human errors, and external events contribute to an increased risk of fraud. This is outlined in the BCBS Principles for the Sound Management of Operational Risk (BCBS, 2011). Furthermore, the research conducted by Cope and Labbi (2012) establishes a clear link between operational risk failures, such as inadequate audits and insider negligence, and incidents of fraud, as detailed in their article (Cope & Labbi, 2012). Power argues that fraudulent events drive investments in mitigation strategies, such as AI monitoring and staff training (Power, 2013).

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1. Introduction

This chapter explains the approach used in gathering and processing data towards the realization of the research objectives. It describes the measures and techniques adopted within the study course, including the type of research plan employed, the different types of data available, the actual source, the population under study, and the tools used to collect data. Again, it goes back in and start dealing with the way the samples are done, how data can be collected, techniques of analysis, and ethical concerns.

3.2. Research Approach

Mixed research method is a comprehensive approach to conducting studies that integrates both qualitative and quantitative research methodologies. Mixed research methods aim to capitalize on the strengths of both approaches, achieving a more robust and well-rounded understanding of the research problem than could be attained using either approach alone (Creswell, 2009). Thus, this study deployed a mixed research method. When the goal is to accurately describe a situation or the relationship between variables, it is essential to choose a design that minimizes bias and maximizes the reliability of the data collected and analyzed (Kothari, 2004).

3.3. Research Design

This study adopted a descriptive research design to investigate and describe the factors contributing to operational risk and financial fraud in commercial banks. The major purpose of descriptive research is a description of the state of affairs as it exists at present, and it includes surveys and fact-finding inquiries of different kinds. The main characteristic of the descriptive approach is that the researcher has no control over the variables and can only report what has happened or what is happening (Kothari, 2004).

3.4. Population and Sample

The study included thirty-one commercial banks, including the Commercial Bank of Ethiopia (CBE) as the country's largest bank, five medium-sized banks, and twenty-five small banks. The next step will be to determine the sample size of the respondent personnel within these institutions. The study focused on key personnel from ethics and anti-corruption, risk

management, internal audit, internal control, and compliance departments. To determine the appropriate sample size, the study employed a purposive sampling technique to ensure the representation of individuals with relevant expertise and exposure to fraud-related activities. The questionnaires will be distributed to two personnel/experts from each department, and it is expected that up to eight personnel from each bank will respond to the questionnaires.

3.5. Data Sources and Types

Data was compiled from primary sources only, as identified in the previous sub-chapter. The questionnaire has been distributed to 31 banks present in the country. In due course, two experts from each department per bank will be selected, totaling 8 respondents per bank (adjusted for smaller banks with limited staff in departments).

3.6. Data Collection Procedure

Different types of research approaches have been employed to study the operational risk in the banking sector in Ethiopia comprehensively. These shall include documentary reviews and questionnaires. Moreover, to mitigate self-reporting bias and enhance data validity, a triangulation approach will be adopted. Details of works are elaborated hereunder:

Documentary Review: A critical review of related literature and reports about the subject provides the necessary background information. This may include regulatory reports (e.g., NBE's Financial Stability Reports, Fraud Monitoring Directives) and document analysis of banks' annual reports and internal audit findings (where publicly available).

Questionnaires: Questionnaires have been distributed to industry experts from all commercial banks in the country, which gives an idea about the subject under study. This has been done by employing structured questionnaires distributed to the stratified sample (as mentioned in previous subchapters).

Most of the literature has underlined the potential of financial fraud to impact banking services, and it highlighted that empirical research is at a nascent stage. The study used a convenient approach to analyze different development, deployment, and impact aspects of operational risk in the Ethiopian banking sector to address the mentioned gap. The methods and techniques, that are employed in conducting the research, are selected and used with full care to widen the avenue for new paths of operational risk research in Ethiopia.

3.7. Ethical Consideration

Ethics can be regarded as the standards of practice that members of a profession or occupation adhere to (Bhattacherjee, 2012). In conducting this research, the confidentiality and privacy of the participants were maintained at all times in strict adherence to ethical procedures. Anonymization through codes such as "Bank A," "Bank B," etc., has been applied to all transcripts to prevent disclosure of individuals or institutions. Participants have been provided with a consent form stating the research's intended use, rights to withdraw at any time, and what confidentiality measures have been instituted. The findings are given as consolidated data in such a manner that no single bank or individual is identified. Ethical clearance authorization has been obtained from the Addis Ababa University School of Commerce to ensure compliance with ethical standards.

3.8. Reliability and Validity

Bryman and Bell highlighted the necessity of performing a pilot study prior to deploying research tools such as self-completion questionnaires or structured interviews. The primary aim of conducting a pilot is not solely to verify the clarity of individual survey questions, but also to ensure that the entire research instrument functions effectively. This process is particularly essential for self-completion questionnaires, as there is no interviewer present to address any confusion that respondents may experience (Bryman & Bell, 2011).

To guarantee reliability, a small group of participants pre-tested the survey instruments. The consistency of their responses was assessed, leading to necessary revisions of the instruments. To establish validity, the research tools were examined by the advisor and field experts. Construct validity was verified through literature reviews to confirm that the instruments accurately measure their intended constructs. As provided by George and Mallery, see Table 3.1, the researcher computed the Cronbach’s alpha value for the instrument and referred to the guidelines (George & Mallery, 2019).

Table 3.1: George and Mallery's Internal Consistency Guideline

Cronbach's alpha	**Internal Consistency**
α≥0.9	Excellent
0.9>α≥0.8	Good
0.8>α≥0.7	Acceptable
0.7>α≥0.6	Questionable
0.6>α≥0.5	Poor
0.5>α	Unacceptable

Source: George and Mallery (2010)

Per the criteria recommended by the above scholars, this study's instrument is in the range of excellent which meant to that the instrument was sufficient enough to measure the intended objective which is evidenced by Table 3.2.

Table 3.2: Reliability Statistics

Cronbach's Alpha	Number of Items
.947	50

Source: Own Survey 2025

3.9. Data Analysis Plan

The mixed-methods design integrates qualitative and quantitative data to provide a comprehensive understanding of the research problem. Qualitative themes identified through thematic analysis of questionnaire transcripts will guide the selection of variables and the development of survey questions for quantitative analysis. This ensures that the quantitative analysis is grounded in qualitative insights, providing a deeper and more contextually relevant

understanding of factors affecting the operational risk of the Ethiopian banking sector. This means that the data analysis entails both qualitative and quantitative approaches, as described below:

Qualitative Approach: Thematic analysis shall be conducted on questionnaire transcripts for the identification of major themes and trends.

Quantitative Approach: Survey data has been cleaned using SPSS, including descriptive statistics.

Moreover, data triangulation has been employed to enhance the validity and reliability of the findings. This involves cross-verifying data from multiple sources, including questionnaire transcripts and secondary documents. This triangulation ensures that the findings are robust and consistent across different data sources, providing a more comprehensive understanding of the research problem.

An integrated data analytical approach will be applied in the present study, and the use of questionnaires will enable qualitative and quantitative analysis. Tools such as SPSS will be useful in the process of data processing with accuracy. Among several statistical methods, various techniques have been chosen to analyze and compare different groups: mean, mean comparison along with cross tabulation, and standard deviations.

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND DISCUSSIONS

4.1. Introduction

In this chapter, we conducted a comprehensive examination and presentation of the data collected during our research. The primary goal of this chapter is to systematically analyze and interpret the data to address the research objectives and answer the research questions outlined in Chapter One. The researcher distributed a structured questionnaire to various departments within the commercial bank, including internal audit, internal control, risk management, compliance, ethics, and anti-corruption employees. This was done to draw conclusions regarding operational risk in Ethiopian commercial banks, with a focus on financial fraud. To gather detailed information, the questionnaire included three fundamental components of operational risk: internal process and system risk, people risk, and external event risk. Additionally, the questionnaire aimed to identify prevalent types of financial fraud committed internally by employees and externally by customers, and potential preventive measures. The study gathered a total of 236 responses from the 248 questionnaires distributed. All responses were collected and organized meaningfully for data processing in SPSS software.

4.2. Response Rate

It can be observed from Table 4.1 that 248 questionnaires were handed out to participants, and 236 of them were filled out and returned, leading to a response rate of 95.16%. The remaining 12 (4.84%) did not respond for different reasons. This strong level of participation increases the representativeness of the data, aiding in the accurate reflection of the perspectives of the target population.

Table 4.1: Response Rate of the Data

Questionnaires	Respondents	Percentage (%)
Distributed	248	100.00
Returned	236	95.16
Unreturned	12	4.84

Source: Own Survey 2025

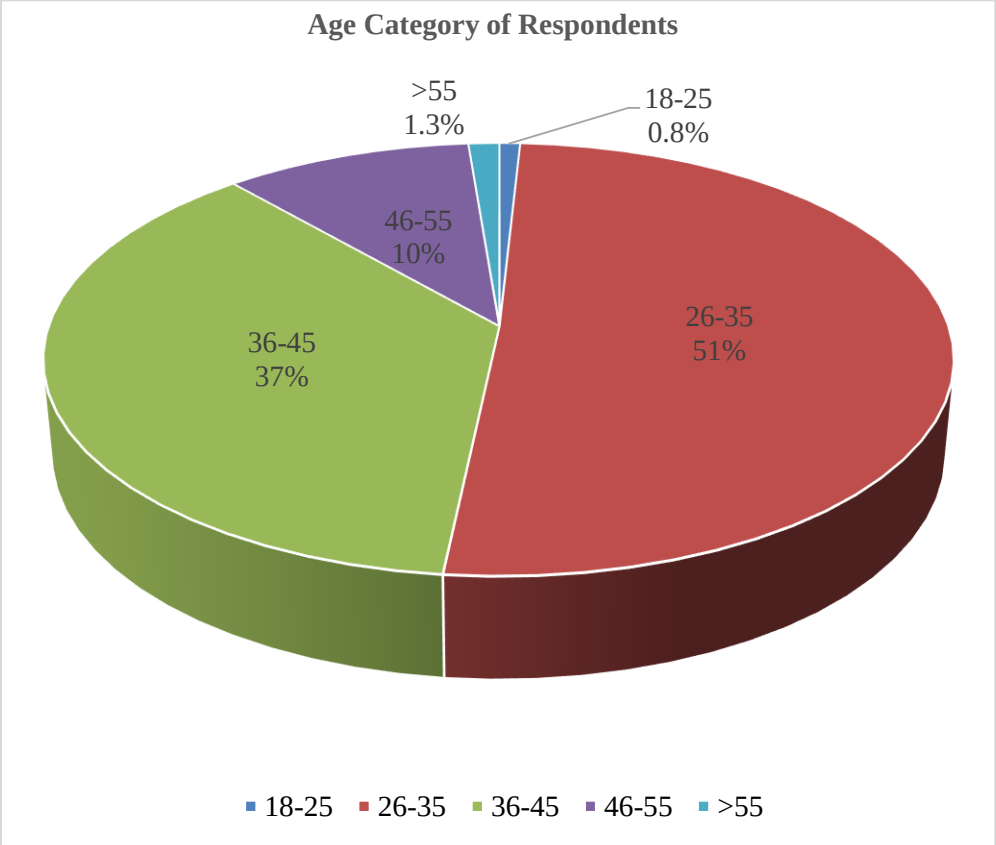
4.3. Demographic Information of the Respondents

The demographic data includes gender distribution, age categories, educational background, work experience, and department.

4.3.1 Age Categories

Figure 4.1 presents the demographic profile of the respondents, providing insights into the characteristics of the study participants. The survey was completed by 236 individuals, of which 50.8 percent were aged between 26 and 35 years, 36.9 percent were between 36 and 45 years, and 10.2 percent were between 46 and 55 years. Additionally, those aged 18 to 25 and above 55 years comprised 0.8 percent and 1.3 percent, respectively.

Figure 4.1: Age Category



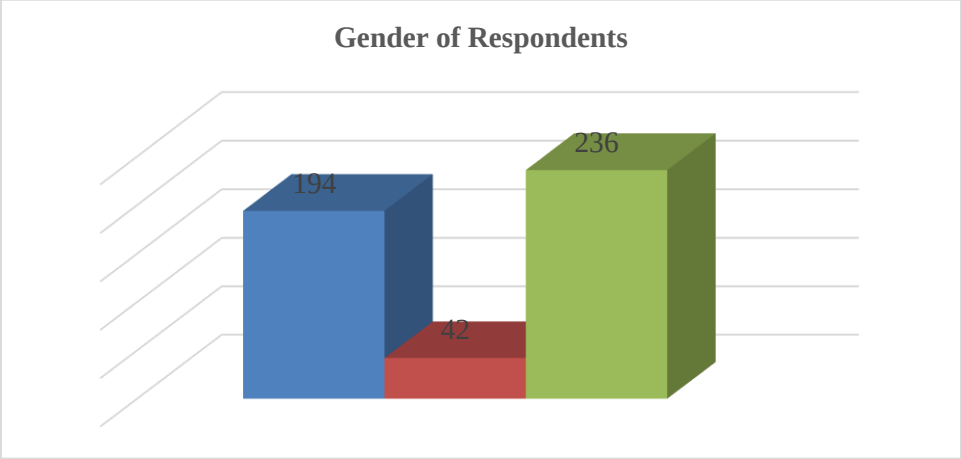
Source: Own Survey 2025

4.3.2 Gender Composition

Figure 4.2 depicts the gender composition of the survey population, which is of special interest according to the analysis. Out of 236 participants, 194 are males and constitute the

majority of the survey population (82.2%), while females are 17.8%. The male-to-female ratio is about 4.6:1.

Figure 4.2: Gender Composition



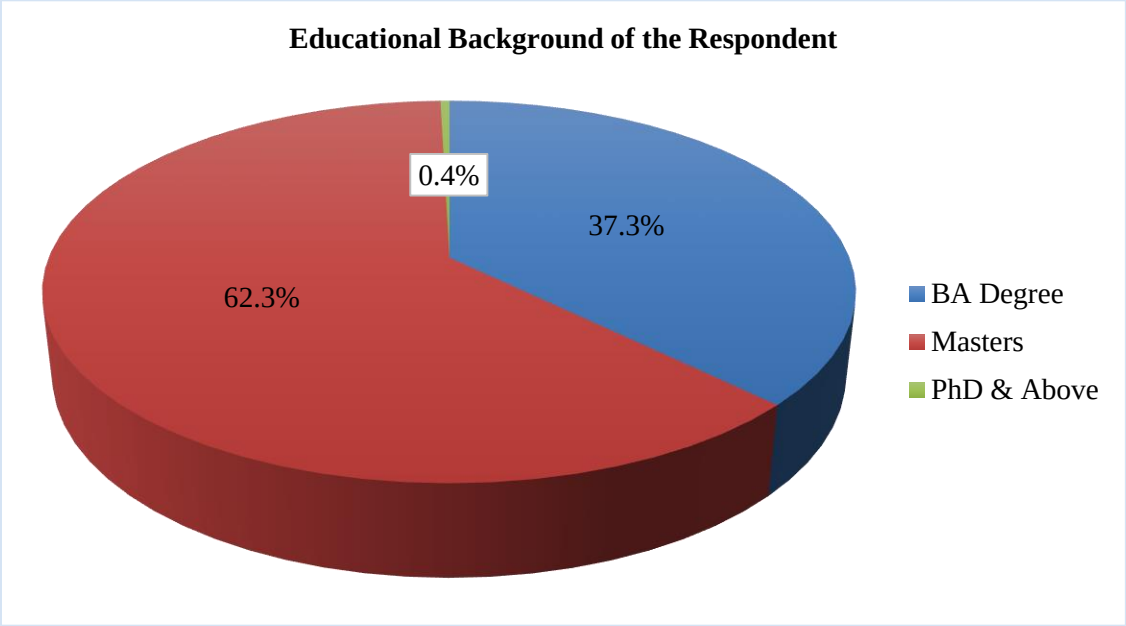
Source: Own Survey 2025

Research published by the World Bank highlights a significant gender imbalance in the banking sector. The study found that only 26 percent of employees at a sample of 18 commercial banks in Ethiopia are women, confirming the existing disparity in representation (Weis, et al., 2022).

4.3.3 Educational Backgrounds of Respondents

The figure below, labeled Figure 4.3: Educational Qualification Distribution, illustrates the educational backgrounds of the respondents. This information is essential for understanding their expertise and perspectives. According to the figure, 62.3 percent of the respondents hold a master's degree, while 37.3 percent have a bachelor's degree, and only 0.4 percent possess a PhD or higher. Thus, the minimum qualification among the respondents is a bachelor's degree. This distribution provides valuable context for analyzing their responses and highlights the diversity of educational attainment within the sample, which may impact their views on the research topic.

Figure 4.3: Educational Background

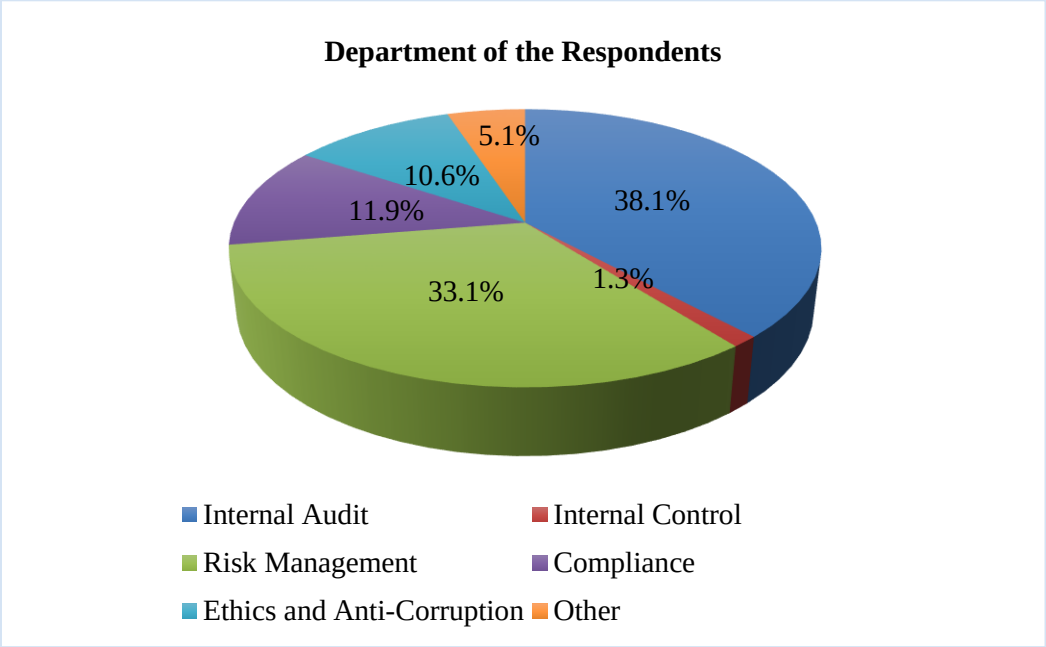


Source: Own Survey 2025

4.3.4 Department of the Respondents

Looking at the department of the respondents in Figure 4.4 below it shows the distribution of respondents across various departments. This breakdown helps us understand the representation of departments in the study, which is essential for capturing diverse perspectives on the topic. As illustrated in the figure, the respondents from internal audit accounted for 38.1 percent, followed by risk management at 33.1 percent. Compliance represented 11.9 percent, ethics and anti-corruption 10.6 percent, others 5.1 percent, and internal control 1.3 percent. This distribution ensures that the study benefits from insights across different functional departments, enriching the analysis and providing a comprehensive understanding of the operational risk in Ethiopian Commercial Banks.

Figure 4.4: Department of the Respondents



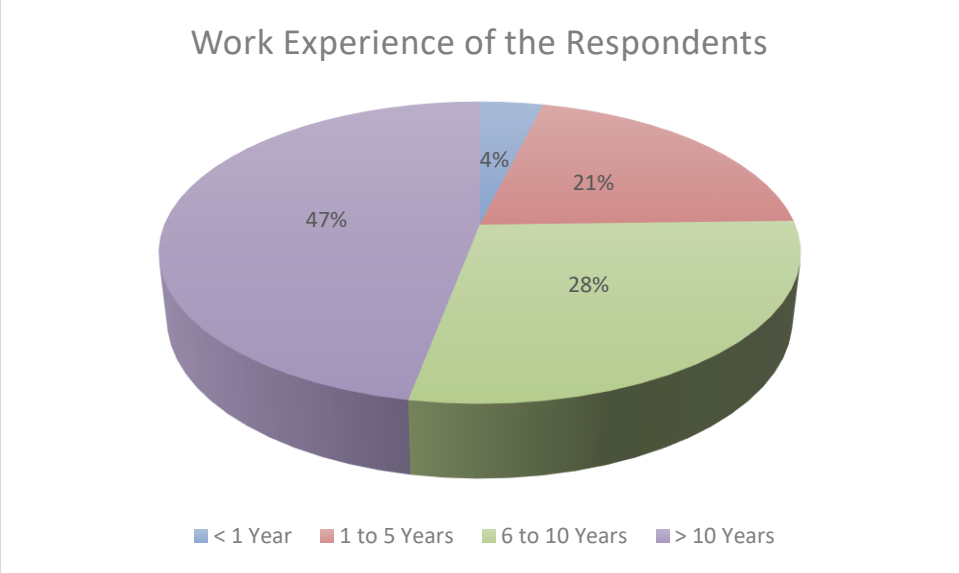
Source: Own Survey 2025

4.3.5 Work Experience of the Respondents

As illustrated in Figure 4.5 below, the majority of respondents, accounting for 47%, possess over 10 years of banking experience. This is followed by those with 6 to 10 years of experience, representing 28.4% of the total. Respondents with 1 to 5 years of experience make up 20.8%, while 3.8% have less than a year of experience. The respondents are highly qualified both academically and professionally.

Notably, as discussed earlier, 62.3% of respondents hold a master's degree, and 47% of respondents have more than 10 years of work experience in the banking industry. This sample comprises individuals well-equipped to provide valuable insights for the study. The combination of advanced education and significant work experience enhances the reliability and depth of the findings derived from their responses.

Figure 4.5: Work Experience



Source: Own Survey 2025

4.4. Internal Processes and Systems

This section presents various internal processes and systems that contribute to operational risk. The survey asked respondents about these internal processes and systems. Figure 4.6 illustrates the responses regarding operational risk using a scale that ranges from "strongly disagree" to "strongly agree."

Concerning the statement, "Lack of segregation of duties increases operational risk and fraud," 52.1% of respondents strongly agreed, while 34.3% agreed. In contrast, 2.5%, 4.2%, and 6.8% of respondents strongly disagreed, disagreed, and chose a neutral response, respectively. A significant majority (86.4%) agreed that the lack of segregation of duties indeed increases operational risk and fraud in commercial banks. This statement received a mean score of 4.29 and a standard deviation of 0.952, suggesting that while most respondents agreed, there was moderate variability in their opinions. This finding aligns with a prior study by Bhasin, which highlighted that clear segregation of duties limits individual control over transactions, thereby reducing opportunities for fraudulent activities (Bhasin, 2015).

In response to the question about the impact of poor documentation practices on operational inefficiencies, 44.1% of respondents strongly agreed, and 43.6% agreed, while 5.9% remained

neutral. Additionally, 3.8% disagreed, and 2.5% strongly disagreed. This indicates that the majority of respondents (87.7%) believe that poor documentation practices do contribute to operational inefficiencies. Most respondents also felt that operational inefficiencies stemming from poor documentation could result in significant risks and potential losses. This perspective received a mean value of 4.23, with a standard deviation of .912, suggesting that there is a general agreement among respondents, although there is moderate variability in their responses. Wells supports this view by explicitly linking poor documentation to the concealment of fraud (Wells, 2017).

Regarding the statement about weak transaction authentication protocols increasing the risk of fraud, the survey results showed that 51.3% of respondents strongly agreed, while 36.9% agreed. Additionally, 5.9% remained neutral, 4.2% disagreed, and 1.7% strongly disagreed. In total, 88.2% of respondents agreed that weak transaction authentication protocols contribute to financial fraud in commercial banks. If a company's policy on transaction authentication is lenient, it may lead to negative outcomes, exposing the organization to the risk of financial loss due to inadequate protocols. This statement received a mean score of 4.32, indicating relatively low variability in responses, meaning most respondents' answers clustered around agreement with less divergence. Specifically, 87.7% of respondents agreed that weak transaction authentication protocols increase the likelihood of financial fraud. This aligns with Joshi's findings, which emphasize that financial institutions with insufficient security measures are more vulnerable to cyber fraud and unauthorized transactions (Joshi, 2022).

The statement "Inadequate IT systems and infrastructure increase operational risks" received significant agreement from survey respondents, with 52.5 percent strongly agreeing and 36 percent agreeing. Meanwhile, 6.4 percent responded neutrally, 3 percent disagreed, and 2.1 percent strongly disagreed. The mean score for this statement was 4.34, with a standard deviation of .887, suggesting that a majority of respondents acknowledged the risks associated with inadequate IT systems and infrastructure. This finding aligns with the observations made by the Basel Committee on Banking Supervision, which emphasizes that outdated or unreliable IT systems can lead to operational failures. Such failures may include transaction errors, system downtimes, and cybersecurity breaches, all of which contribute to increased operational risk. Reference: Basel Committee on Banking Supervision (BCBS, 2011).

In relation to the statement, "Manual processes are a significant source of operational risk," 41.5 percent of respondents agreed, and 25 percent strongly agreed. Meanwhile, 22 percent remained neutral, 9.3 percent disagreed, and 2.1 percent strongly disagreed. This statement received a mean value of 3.78, with a standard deviation of 0.995, indicating a general agreement among respondents with moderate variation in their responses. This consensus aligns with the Basel Committee on Banking Supervision, which identifies manual processes, such as data entry and reconciliations, as prone to errors, fraud, and inefficiencies, thus increasing operational risk (BCBS, 2011).

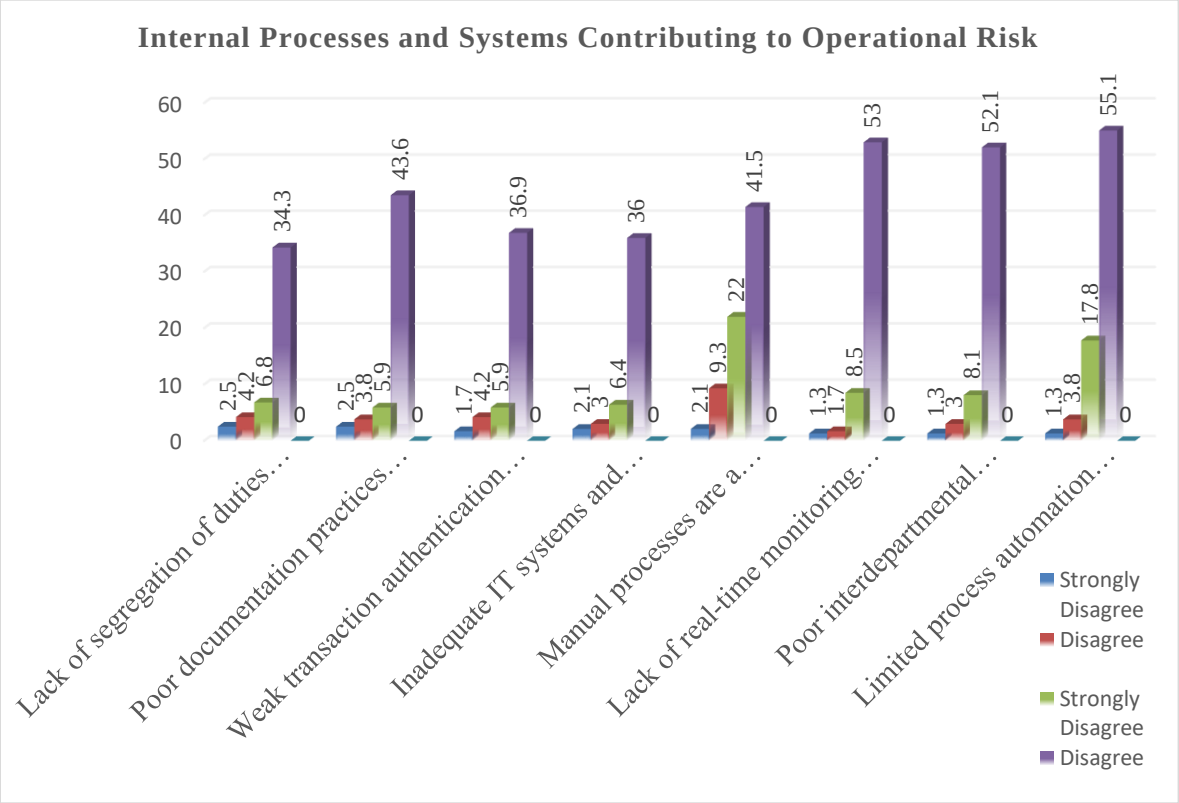
Regarding the statement, "Lack of real-time monitoring systems increases fraud risks," 53 percent of respondents agreed, and 35.6 percent strongly agreed. Additionally, 8.5 percent were neutral, while 1.7 percent disagreed, and 1.3 percent strongly disagreed. On average, respondents expressed strong agreement with this statement (mean = 4.20), with most ratings falling between 3.4 and 5. The moderate standard deviation (0.765) suggests some minor disagreement, but the overall sentiment remains highly positive. Specifically, 88.6 percent of respondents concurred that the lack of real-time monitoring systems increases fraud risks. This is supported by a study from Deloitte, which found that 78 percent of payment fraud cases at banks could have been prevented through real-time transaction screening (Deloitte, 2023).

The statement "poor interdepartmental communication leads to operational inefficiencies" received a significant level of agreement from respondents, with 52.1% agreeing and 35.6% strongly agreeing. In contrast, 8.1% responded neutrally, while 3% disagreed and 1.3% strongly disagreed. This statement had a mean score of 4.18 and a standard deviation of 0.800, indicating a high level of agreement among participants, along with moderate variation in their responses. Supporting this, a study by IBM found that organizations with strong cross-department communication report a 35% faster time-to-market and 50% fewer operational errors (Deloitte, 2023).

Regarding the statement "limited process automation increases operational risks," 55.1% of respondents agreed and 22% strongly agreed. Additionally, 17.8% remained neutral, while 3.8% disagreed and 1.3% strongly disagreed. This statement received a mean score of 3.93 and a standard deviation of 0.814, suggesting general agreement among respondents, with moderate variation in their responses. This finding aligns with Basel’s report, which identifies

manual processes as significant vulnerabilities, noting that 68% of operational risk events in banks stem from non-automated workflows (BCBS, 2021).

Figure 4.6: Internal Processes and Systems Contributing to Operational Risk



Source: Own Survey 2025

Inadequate IT systems and infrastructure, weak transaction authentication protocols, and a lack of segregation of duties are identified as the most critical factors, as shown in Table 4.2. In contrast, manual processes are considered moderate factors and represent a significant source of concern compared to the other issues. Most factors have mean around 4 which shows general agreement.

Table 4.2: Mean Comparison across Internal Processes and Systems

Mean Comparison across Internal Processes and Systems		
Internal Processes and Systems	Mean	Std. Deviation
Lack of segregation of duties increases operational risk and fraud	4.29	0.952
Poor documentation practices contribute to operational inefficiencies	4.23	0.912
Weak transaction authentication protocols increase fraud risks	4.32	0.892
Inadequate IT systems and infrastructure increase operational risks	4.34	0.887
Manual processes are a significant source of operational risk	3.78	0.995
Lack of real-time monitoring systems increases fraud risks	4.20	0.765
Poor interdepartmental communication leads to operational inefficiencies	4.18	0.800
Limited process automation increases operational risks	3.93	0.814
Average	4.16	0.877

Source: Own Survey 2025

4.5. Human Factors

This section, as depicted in Figure 4.7 below, evaluates the role of human factors (e.g., employee behavior, training) in operational risk. With the statement "Lack of employee training increases operational risk and fraud," respondents were asked to share their opinions. A total of 52.5% agreed and 39% strongly agreed, while 5.9% remained neutral, 1.7% disagreed, and 0.8% strongly disagreed. The majority of respondents (91.5%) acknowledged that a lack of employee training contributes to operational risk and fraud. They believed that when employees are not adequately equipped with the tools to prevent and detect fraudulent activities, the associated risks and potential losses can be significant. This statement received a mean value of 4.27, with a standard deviation of .722, indicating that most respondents agree that insufficient employee training significantly contributes to operational risk and fraud, with moderate variation in responses. This finding aligns with Bhasin's study, which emphasizes

that employee training and awareness programs should incorporate fraud awareness. Without proper training, employees may struggle to identify fraudulent transactions, thereby increasing the organization's vulnerability (Bhasin, 2015).

Regarding the statement "high employee turnover rates contribute to operational inefficiencies," respondents were asked to share their opinions. The results showed that 53.4% agreed, 30.1% strongly agreed, 12.7% were neutral, while 3% and 0.8% disagreed and strongly disagreed, respectively. This question was posed to gather insights on the issue at hand. The majority of respondents (83.5%) acknowledged that high employee turnover rates contribute to operational inefficiencies. When employees leave the company, especially due to grievances and dissatisfaction, they may take advantage of their knowledge and experience, potentially colluding with current employees against the organization. The mean score of 4.09 and a standard deviation of .786 indicate a moderate level of agreement among respondents, suggesting that high employee turnover is recognized as a factor contributing to operational inefficiencies. This finding aligns with McKinsey & Company's report, which states that organizations with high turnover experience 18% more process errors (due to knowledge gaps) and 27% lower customer satisfaction (due to inconsistency) (McKinsey & Company, 2022).

Employee misconduct is a significant source of financial fraud. In a survey, 45.8 percent of respondents agreed with this statement, while 38.1 percent strongly agreed. Additionally, 12.7 percent were neutral, 2.1 percent disagreed, and 1.3 percent strongly disagreed. The statement received a mean score of 4.17 and had a standard deviation of .825, indicating a general agreement among respondents, though there was some variability in their responses. Overall, 83.9 percent of respondents agreed with the statement. These findings support the prior study by the ACFE, which states that employee misconduct is the root cause of 86% of occupational fraud cases. The primary categories of fraud include financial statement fraud, asset misappropriation, and corruption (ACFE, 2024).

The statement regarding "insufficient background checks during employee hiring increasing fraud risks" received significant feedback from respondents. Specifically, 46.6 percent agreed, 39 percent strongly agreed, 11.9 percent were neutral, 2.1 percent disagreed, and 0.4 percent strongly disagreed. Overall, the majority of respondents (85.6%) acknowledged that inadequate employee background checks during hiring contribute to financial fraud in

commercial banks. If a company's hiring policy is weak, it can lead to negative outcomes, as employees may present forged academic qualifications and may have problematic prior employment histories. This statement received a mean score of 4.22 and a standard deviation of .766, indicating that respondents perceive insufficient employee background checks during hiring as a significant factor in fraud risks, with moderate variability in their opinions. This finding aligns with the research by Zahra and her colleagues, which emphasizes that an employee's background plays a crucial role in influencing their likelihood of committing fraud. Weak hiring processes create opportunities for individuals with fraudulent histories to enter the organization, increasing the risk of fraud (Zahra, et al., 2007).

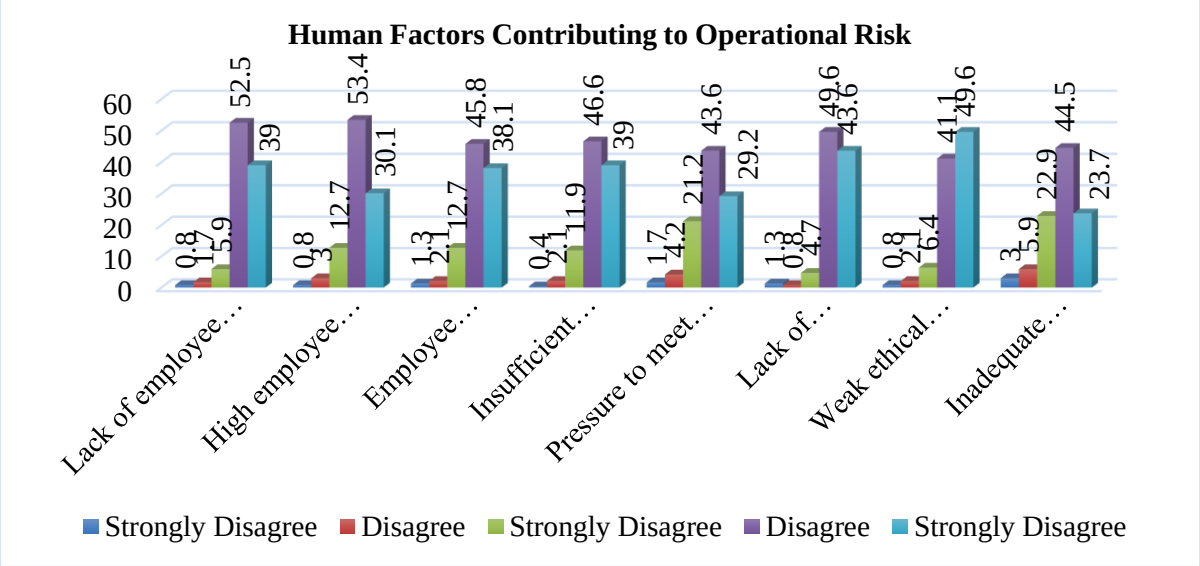
In the context of the pressure to meet financial targets leading to fraudulent activities, a survey of respondents revealed that 72.8% believe this pressure drives employees to engage in fraud, resulting in financial misconduct. Specifically, 43.6% of respondents agreed, while 29.2% strongly agreed. Additionally, 21.2% of respondents remained neutral, and 4.2% disagreed, with 1.7% strongly disagreeing. The mean score of 3.94 and a standard deviation of .909 indicate a moderate agreement that pressure to achieve financial goals fosters an environment conducive to fraudulent activities, as employees may resort to illegal methods to meet expectations. Excessive pressure can lead to unethical behavior, including the manipulation of financial records to create misleading performance results. This notion is supported by the ACFE's report, which identifies excessive pressure to meet financial or sales targets as one of the three key elements of the Fraud Triangle, creating an incentive for employees to commit occupational fraud (ACFE, 2024).

Concerning the lack of accountability and oversight increasing operational risks, 49.6 percent of respondents agreed, while 43.6 percent strongly agreed. Additionally, 4.7 percent chose a neutral response, 0.8 percent disagreed, and 1.3 percent strongly disagreed. The overwhelming majority of responses (93.2%) indicate that a lack of clear accountability and oversight heightens the likelihood of operational risks. This statement received a mean score of 4.33 with a standard deviation of .722, suggesting that poor accountability and oversight significantly contribute to operational risks, albeit with moderate variability among respondents. This finding aligns with previous studies that indicate weak internal controls and a lack of accountability create opportunities for fraudulent activities (Joshi, 2022). Regarding the statement, "Weak ethical culture within the organization encourages misconduct," 49.6 percent

of respondents strongly agreed, and 41.1 percent agreed. Additionally, 6.4 percent responded neutrally, while 2.1 percent disagreed and 0.8 percent strongly disagreed. Based on these survey results, the mean score for the statement was 4.36, with a standard deviation of .768. This indicates that a majority of respondents agreed with the statement, though there was some variation in responses. This result is consistent with the Ethics & Compliance Initiative's (ECI) survey, which found that organizations with weak ethical cultures experience rates of misconduct 10 times higher than those with strong cultures, as employees perceive fewer consequences for unethical behavior (ECI, 2023).

The statement "Inadequate incentive structures represent a measurable fraud risk factor within organizations" received significant feedback from respondents. Specifically, 44.5% of participants agreed with the statement, while 23.7% strongly agreed. The remaining responses included 22.9% who were neutral, 5.9% who disagreed, and 3% who strongly disagreed. The statement resulted in a mean value of 3.80, with a standard deviation of 0.967, indicating a moderate level of agreement among respondents and moderate variation in their responses. According to the ACFE, poorly designed incentive programs—especially those that focus heavily on short-term financial targets—are a measurable fraud risk factor present in 31% of occupational fraud cases (ACFE, 2024).

Figure 4.7: Human Factors Contributing to Operational Risk



Source: Own Survey 2025

As shown in Table 4.3, the statement "Weak ethical culture within the organization encourages misconduct" received the highest mean score of 4.36, indicating strong agreement among respondents and relatively moderate variability in their responses. In contrast, the statement "Inadequate incentive structures represent a measurable fraud risk factor within organizations" had the lowest mean score of 3.80, with the highest variability in responses. Most of the other factors had mean scores clustered around 4, indicating a general consensus on these statements.

Table 4.3: Mean Comparison across Human Factors

Mean Comparison across Human Factors		
Human Factors	Mean	Std. Deviation
Lack of employee training increases operational risk and fraud	4.27	0.722
High employee turnover rates contribute to operational inefficiencies	4.09	0.786
Employee misconduct is a significant source of financial fraud	4.17	0.825
Insufficient background checks during hiring increase fraud risks	4.22	0.766
Pressure to meet financial targets leads to fraudulent activities	3.94	0.909
Lack of accountability and oversight increases operational risks	4.33	0.722
Weak ethical culture within the organization encourages misconduct	4.36	0.768
Inadequate incentive structures represent a measurable fraud risk factor within organizations	3.80	0.967
Average	4.15	0.808

Source: Own Survey 2025

4.6. External Factors

This section is dedicated to analyzing the influence of external factors (e.g., regulatory environment, emerging technologies, and third-party vendors), as can be seen in Figure 4.8, on operational risk. With the statement, "Weak enforcement of compliance standards increases operational risks," 58.9 percent of respondents agreed, and 28.8 percent strongly agreed. Additionally, 7.6 percent remained neutral, while 3.8 percent disagreed and 0.8 percent

strongly disagreed. Overall, 87.7 percent of the total respondents agreed that weak enforcement of compliance standards leads to increased operational risks in commercial banks. This statement received a mean score of 4.11, with a standard deviation of .764, indicating a high level of agreement among respondents, accompanied by moderate variability. This aligns with the International Organization for Standardization (ISO), which states that failure to effectively enforce compliance policies can result in non-conformities, leading to operational inefficiencies and heightened risks (ISO, 2021).

Regarding the statement that "Outdated regulatory frameworks contribute to financial fraud," 56.8 percent of respondents agreed, and 21.6 percent strongly agreed. In addition, 15.7 percent were neutral, while 5.5 percent disagreed and 0.4 percent strongly disagreed. Therefore, 78.4 percent of respondents believe that outdated regulatory frameworks facilitate financial fraud. This statement received a mean value of 3.94 and a standard deviation of .794, indicating a strong acknowledgment of the role that outdated regulatory frameworks play in enabling financial fraud, despite some moderate divergence in opinions. This finding aligns with the World Bank's report, which states that weak or obsolete financial regulations increase systemic vulnerabilities, thereby enabling fraud and illicit financial flows (World Bank, 2020).

About the statement, "The lack of specialized oversight for emerging technologies increases risks," a total of 56.8 percent of respondents agreed, while 31.4 percent strongly agreed. Meanwhile, 9.7 percent of participants were neutral, 1.7 percent disagreed, and 0.4 percent strongly disagreed. Overall, 88.2 percent of respondents believe that the absence of specialized oversight for emerging technologies escalates risks. This statement received a mean score of 4.17 and a standard deviation of 0.700, indicating a strong perception that the lack of specialized regulatory oversight for emerging technologies is a significant factor contributing to increased risks, with higher agreement and moderate variability among participants. Supporting this view, the U.S. Government Accountability Office (GAO) highlighted that the absence of specialized oversight mechanisms for emerging technologies, such as AI and blockchain, raises concerns related to security, fraud, and financial stability (GAO, 2023).

Regarding the statement, "Inconsistent enforcement of anti-fraud regulations increases fraud risks," 55.1 percent of respondents agreed, and 30.1 percent strongly agreed. Additionally, 10.6 percent were neutral, 3.8 percent disagreed, and 0.4 percent strongly disagreed. Thus, 85.2

percent of respondents perceive inconsistent enforcement of anti-fraud regulations as a contributing factor to fraud risks. This statement received a mean score of 4.11 and a standard deviation of .767, indicating that inconsistent enforcement is recognized as a significant issue, with moderate variability among respondents. This finding aligns with the ACFE's report, which confirms a direct correlation between inconsistent enforcement of anti-fraud regulations and increased fraud risks, as it creates opportunities for exploitation (ACFE, 2022).

The statement "Regulatory bodies lack sufficient resources to combat fraud effectively" received significant responses from participants. Specifically, 44.1% of respondents agreed, while 20.8% strongly agreed. In addition, 26.7% remained neutral, 6.8% disagreed, and 1.7% strongly disagreed. Overall, 64.9% of respondents perceived insufficient resources for regulatory bodies as a notable factor contributing to fraud. This statement garnered a mean value of 3.75 with a standard deviation of 0.917, indicating that the lack of sufficient resources in regulatory bodies contributes to fraud risks, with moderate variability in opinions among respondents. This finding aligns with Bhasin's study, which highlighted that regulatory agencies often lack the financial and human resources necessary for thorough investigations and effective enforcement of penalties (Bhasin, 2016).

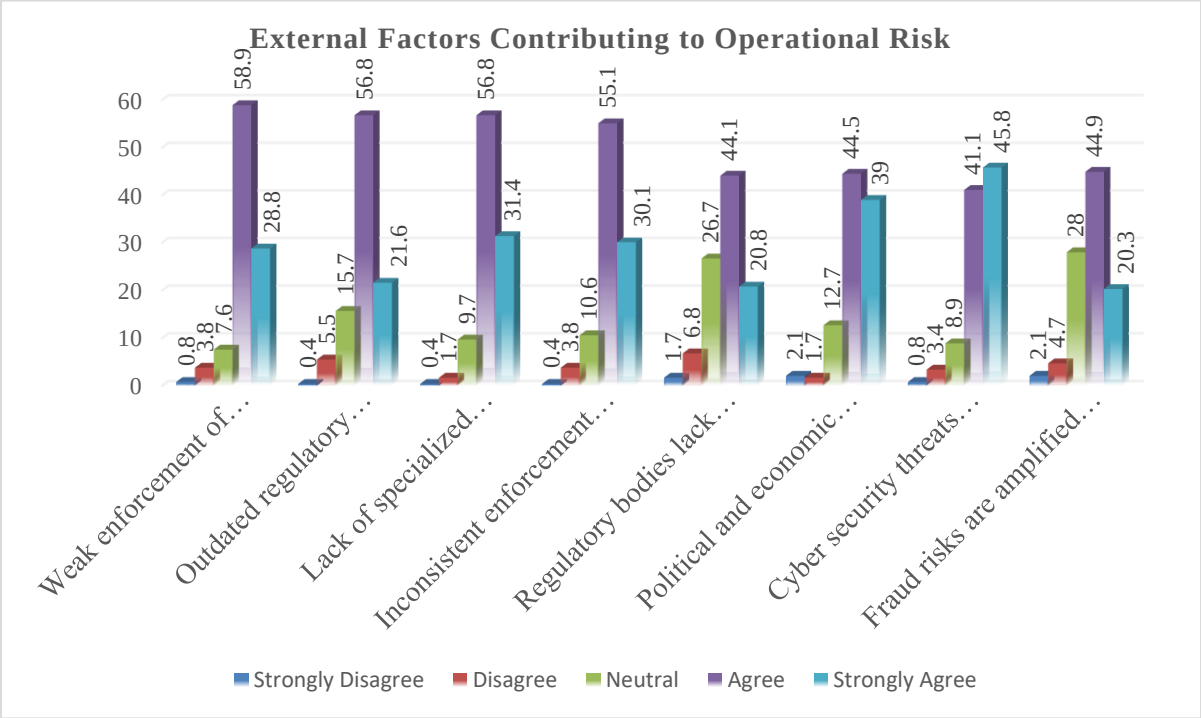
Regarding the statement "Political and economic instability exacerbate operational risks," 44.5% of respondents agreed and 39% strongly agreed. Furthermore, 12.7% remained neutral, while 1.7% disagreed and 2.1% strongly disagreed. A majority of 83.5% of respondents acknowledged that political and economic instability significantly exacerbates operational risks. The mean score for this statement was 4.17, with a standard deviation of .867, indicating strong agreement among respondents. This suggests that political and economic instabilities are widely recognized as significant factors contributing to operational risks, even though there is moderate variability in opinions. The World Bank confirmed in its report that political turmoil and economic volatility directly increase operational risks for businesses by disrupting supply chains, weakening institutions, and escalating security threats (World Bank, 2022).

In response to the statement "Cybersecurity threats (e.g., hacking) pose significant operational risks," 45.8 percent of respondents strongly agreed, while 41.1 percent agreed. In contrast, 8.9 percent remained neutral, 3.4 percent disagreed, and 0.8 percent strongly disagreed. Overall, 86.9 percent of the respondents indicated that cybersecurity threats, such as hacking, greatly

increase operational risks in commercial banks. This statement received a mean score of 4.28, with a standard deviation of .828, indicating strong agreement among respondents, although there was moderate variability in their responses. According to a report by GAO cybersecurity threats, including hacking and ransomware attacks, pose significant operational risks to critical infrastructure and financial systems (GAO, 2023).

Regarding the statement "Fraud risks are amplified due to inadequate third-party vendor risk management," 44.9 percent of respondents agreed, 20.3 percent strongly agreed, 28 percent remained neutral, 4.7 percent disagreed, and 2.1 percent strongly disagreed. The majority of respondents (65.2 percent) agreed that inadequate third-party vendor risk management amplifies fraud risks in commercial banks. The statement received a mean score of 3.7669, indicating moderate consensus among respondents, with a standard deviation of 0.89960, reflecting consistent responses but also moderate variability. This finding is supported by a report from the Association of Certified Fraud Examiners, which states that organizations with weak third-party risk management programs experience 40 percent higher fraud losses due to vendor-related schemes (ACFE, 2022).

Figure 4.8: External Factors Contributing to Operational Risk



Source: Own Survey 2025

As illustrated in Table 4.4, cybersecurity threats have the highest mean score of 4.28, indicating strong agreement among respondents regarding their status as a critical factor. The standard deviation of 0.828 suggests a moderate level of consensus. Conversely, the statement about regulatory bodies lacking sufficient resources to effectively combat fraud received the least agreement, with a mean score of 3.7 and the highest variability in responses, as reflected by a standard deviation of 0.917.

Table 4.4: Mean Comparison across External Factors

Mean Comparison across External Factors		
External Factors	Mean	Std. Deviation
Weak enforcement of compliance standards increases operational risks	4.11	0.764
Outdated regulatory frameworks contribute to financial fraud	3.94	0.794
Lack of specialized oversight for emerging technologies increases risks	4.17	0.700
Inconsistent enforcement of anti-fraud regulations increases fraud risks	4.11	0.767
Regulatory bodies lack sufficient resources to combat fraud effectively	3.75	0.917
Political and economic instability exacerbate operational risks	4.17	0.867
Cyber security threats (e.g., hacking) pose significant operational risks	4.28	0.828
Fraud risks are amplified due to inadequate third-party vendor risk management	3.77	0.900
Average	4.04	0.817

Source: Own Survey 2025

4.7. Types of Financial Fraud

This section identifies the prevalent types of financial fraud committed by customers and employees. The areas this study would like to see for prevalent types of financial fraud committed by customers are Identity Theft, Cheque Fraud, Debit Card Fraud, Mobile Banking Fraud, Phishing Scams, Money Laundering, and Terrorist Financing. For prevalent types of financial fraud committed by employees, the following factors: Embezzlement, Bribery,

Collusion With External Parties, Debit From Dormant Accounts, Transaction Reversal Fraud, Cashier Payment Order Fraud, Corruption, Debit From Deceased Customer's Account, and Opening Fraudulent Accounts.

4.7.1 Prevalent Types of Financial Fraud Committed by Customers

This part is committed for prevalent types of financial fraud committed by customers as depicted in Figure 4.9. Concerning identity theft, a prevalent type of financial fraud among customers in commercial banks, 40.7 percent of respondents rated their concern as high, 24.2 percent as moderate, 16.9 percent as very high, 12.3 percent as low, and 5.9 percent as not concerned at all. This statement received a mean score of 3.50 and a standard deviation of 1.093, indicating that identity theft is recognized as a significant issue, with 57.6 percent of respondents perceiving it as high overall. There is some variation in perceptions among respondents. This supports with prior studies by Bhasin, Joshi, and Setarge, which highlight identity theft as a major challenge in the banking sector, as fraudsters exploit stolen personal information to gain unauthorized access to accounts (Bhasin, 2015) (Joshi, 2022) (Setarge, 2022).

Regarding the statement, "cheque fraud is one of the prevalent types of financial fraud committed by customers in commercial banks," 43.6 percent of respondents rated it as high, 22.9 percent as moderate, 22.5 percent as very high, 8.9 percent as low, and 2.1 percent as not at all concerned. This statement received a mean score of 3.75 and a standard deviation of 0.971, indicating that cheque fraud is perceived as highly prevalent, with a clear tendency towards the higher end of the scale. Most respondents rated cheque fraud consistently as high, with 66.1 percent identifying it as high or very high, showing limited variation in responses. This aligns with the findings of Gebreselasie, who identified cheque fraud as a persistent issue in commercial banking (Gebreselasie, 2022).

Debit card fraud is a prevalent type of financial fraud committed by customers in commercial banks. In a recent survey, 34.3% of respondents rated the level of debit card fraud as high, 33.9% as moderate, 14% as low, 11.4% as very high, and 6.4% as not at all. The mean score of 3.31, along with a standard deviation of 1.052, suggests that debit card fraud is perceived as moderately to highly prevalent, leaning slightly towards high with moderate variation among respondents. This finding brings into line with previous research indicating that card skimming

and unauthorized transactions are significant security concerns in card-based banking (Setarge, 2022).

Regarding the statement "mobile banking fraud is the most prevalent type of financial fraud committed by customers in commercial banks," 41.5% of respondents rated it as very high, 36.9% as high, 11% as moderate, 7.2% as low, and 3.4% as not at all. The mean score of 4.06 and a standard deviation of 1.058 indicate that mobile banking fraud is perceived as highly prevalent, with 78.4% of respondents rating it as high or very high. This reflects a strong consensus among participants and suggests a moderate level of agreement among them. These results are consistent with studies by Bhasin and Setarge, which identify mobile banking fraud as a growing challenge in digital banking security (Bhasin, 2016) (Setarge, 2022).

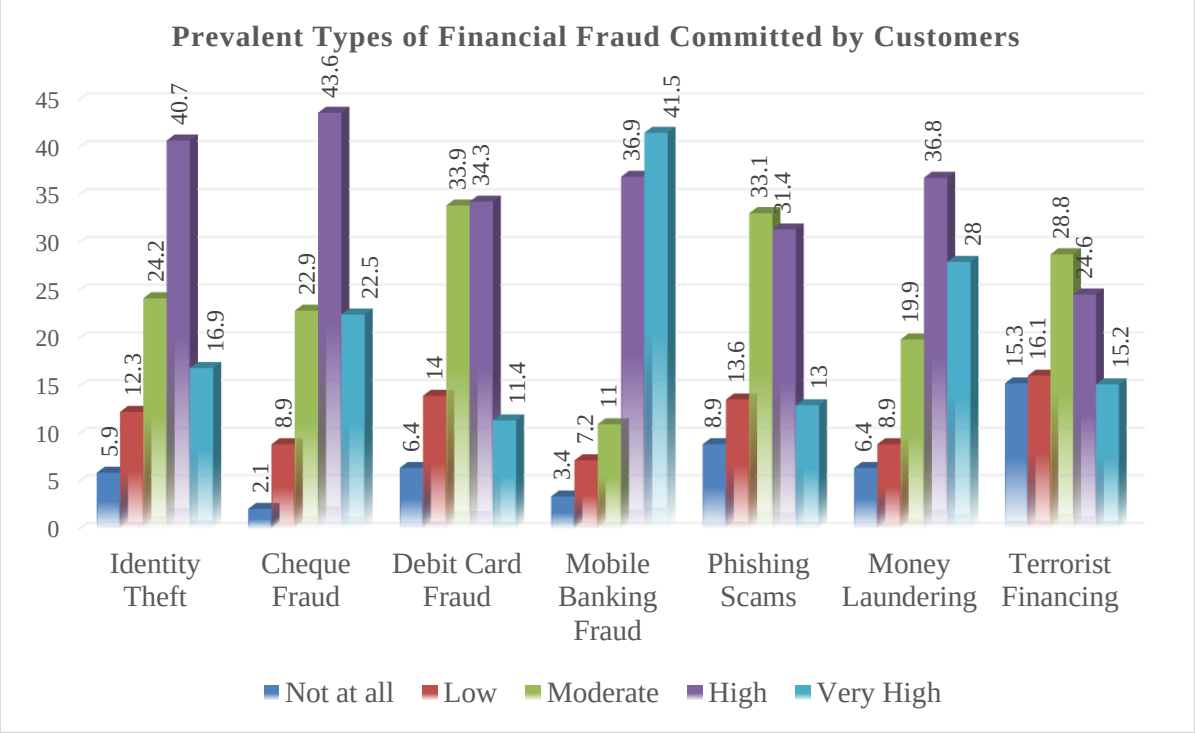
In relation to phishing scams, which is a prevalent type of financial fraud committed by customers in commercial banks, 33.1% of respondents rated its prevalence as moderate, 31.4% as high, 13.6% as low, 13.1% as very high, and 8.9% as not at all. The mean score of 3.2627, along with a standard deviation of 1.12555, suggests that phishing scams are perceived as moderately prevalent, though closer to the lower end of the scale, indicating relatively moderate variation in responses. Worku identified phishing as a significant type of fraud; however, the variability in responses implies that its impact may vary across different banking institutions (Worku, 2020).

Regarding the statement ‘money laundering is the prevalent type of financial fraud committed by customers in commercial banks’, 36.9% of respondents rated it as high, 28% as very high, 19.9% as moderate, 8.9% as low, and 6.4% as not at all. This statement received a mean score of 3.71 and a standard deviation of 1.153, indicating that money laundering is considered fairly prevalent as a type of financial fraud, with moderate variation among respondents. This finding aligns with the Financial Action Task Force (FATF) study, which states that commercial banks remain the most vulnerable sector for money laundering due to their high transactional volume and global reach (FATF, 2022).

Concerning terrorist financing, a significant type of financial fraud committed by customers in commercial banks has been identified. According to survey results, 28.8 percent of respondents rated the prevalence of this issue as moderate, 24.6 percent as high, 16.1 percent as low, and 15.3 percent each as very high and not at all. This statement received a mean score of 3.08,

with a standard deviation of 1.275. This suggests that terrorist financing is perceived as being low to moderately prevalent, with considerable variation among respondents. This finding is supported by a study from the Financial Action Task Force (FATF), which notes that although less frequent than money laundering, terrorist financing remains a critical risk in commercial banks. It accounts for 12-18% of suspicious transaction reports (STRs) linked to customer activity in high-risk jurisdictions (FATF, 2023).

Figure 4.9: Prevalent Types of Financial Fraud Committed by Customers



Source: Own Survey 2025

As illustrated in Table 4.5, mobile banking fraud is the most common type of financial fraud, and there is a strong consensus among respondents about this issue. In contrast, terrorist financing is viewed as the least common type of fraud, with responses showing greater variability. Additionally, debit card fraud and phishing scams are also regarded as less prevalent forms of fraud.

Table 4.5: Mean Comparison across Types of Financial Fraud Committed by Customers

Mean Comparison across Types of Financial Fraud Committed by Customers		
Types of Financial Fraud Committed by Customers	Mean	Std. Deviation
Identity Theft	3.50	1.093
Cheque Fraud	3.75	0.971
Debit Card Fraud	3.31	1.052
Mobile Banking Fraud	4.06	1.058
Phishing Scams	3.26	1.126
Money Laundering	3.71	1.153
Terrorist Financing	3.08	1.275
Average	3.53	1.104

Source: Own Survey 2025

4.7.2 Prevalent Types of Financial Fraud Committed by Employees

This section is designated, as shown in Figure 4.10, for interpreting the prevalent types of financial fraud committed by employees. Regarding the statement that "embezzlement is the prevalent type of financial fraud committed by employees in commercial banks," 39.4 percent of respondents rated it as high, 24.6 percent as moderate, 22.5 percent as very high, 8.1 percent as low, and 5.5 percent as not at all. This statement received a mean score of 3.65 and a standard deviation of 1.083, indicating that the majority of respondents believe embezzlement is indeed a prevalent type of financial fraud committed by employees, with moderate variation in their responses. This finding is supported by a World Bank report, which highlights that internal fraud, particularly embezzlement, poses a significant risk in commercial banks. This often involves tellers, loan officers, and accountants manipulating transactions (World Bank, 2016).

Regarding the statement that "bribery is the prevalent type of financial fraud committed by employees in commercial banks," 42.4 percent of respondents rated it as high, 23.7 percent as moderate, 17.4 percent as very high, 10.6 percent as low, and 5.9 percent as not at all. This statement received a mean score of 3.55 and a standard deviation of 1.081, indicating that the majority of respondents view bribery as a prevalent type of financial fraud committed by employees, with moderate variability in their responses. This result is also reflected in a World Bank study, which indicates that in many emerging markets, bribery and kickbacks are the

most common forms of corruption in commercial banks, particularly concerning loan approvals, procurement, and regulatory evasion (World Bank, 2019).

The statement "collusion with external parties is the most common type of financial fraud committed by employees in commercial banks" received varied responses. Specifically, 38.1% of respondents rated it as high, 27.5% as moderate, 17.4% as very high, 10.6% as low, and 6.4% indicated it was not prevalent at all. Cumulatively, 83% of respondents view collusion with external parties as at least moderately prevalent. This statement achieved a mean score of 3.50, with a standard deviation of 1.093, reflecting a strong tendency toward agreement among respondents and a consistent pattern in their responses. This trend is supported by ACFE, which highlights that collusion between bank employees and external actors—such as clients and vendors—accounts for 42% of high-loss fraud cases in financial institutions, outpacing incidents of solo-employee theft (ACFE, 2024).

The statement "debit from dormant accounts is the most common type of financial fraud committed by employees in commercial banks" received significant attention in a recent survey. Among the respondents, 37.7% rated this type of fraud as high in prevalence, while 28.4% rated it as very high. Additionally, 15.3% considered it to be moderate, 11.4% ranked it as low, and 7.2% said it was not prevalent at all. Overall, 81.4% of respondents believe that this type of financial fraud is at least moderately common. The statement received a mean score of 3.69, with a standard deviation of 1.204, indicating a moderate tendency toward agreement and a moderate level of variation in the responses. This finding aligns with a case study that analyzed bank fraud in Nigeria and Kenya over six years and revealed that 68% of internal fraud incidents involved employees siphoning funds from dormant accounts, often due to weak reconciliation processes. This reflects the serious implications of dormant account fraud in the banking sector (Adeoye & Rahman, 2020).

Transaction reversal fraud is the most common type of financial fraud committed by employees in commercial banks. According to survey results, 37.3% of respondents rated it as a high concern, 24.2% as moderate, 11.9% as very high, 17.8% as low, and 8.9% as not at all concerning. Overall, the majority of respondents (73.4%) perceive transaction reversal fraud as, at the very least, a moderate issue in commercial banks. This statement received a mean score of 3.25 and a standard deviation of 1.150, indicating a moderate level of agreement and

variation in responses. Additionally, a survey conducted by the Federal Financial Institutions Examination Council's (FFIEC) report on bank fraud trends highlighted a significant rise in transaction reversal fraud. Examiners observed that employees often exploit system glitches or override controls to reverse legitimate transactions into fraudulent accounts (FFIEC, 2022).

In the context of Cashier Payment Order (CPO) Fraud, this type of financial fraud is notably prevalent among employees in commercial banks. According to survey results, 36.9 percent of respondents rated the occurrence of CPO Fraud as high, 22 percent as moderate, 20.3 percent as low, 14.4 percent as very high, and 6.4 percent as not at all. The cumulative percentage of 73.3 percent indicates that respondents perceive Cashier Payment Order Fraud as at least moderately prevalent, with a mean score of 3.33 and a standard deviation of 1.141. This reflects a general trend towards moderate agreement and a consistent distribution of responses. A report by Bangladesh Bank highlights the prevalence of such fraudulent activities in commercial banks, revealing that Cashier Payment Order (CPO) fraud accounted for 38% of internal fraud cases in 2022. This primarily involves bank staff forging authorized signatures or manipulating manual payment systems (Bangladesh Bank, 2023).

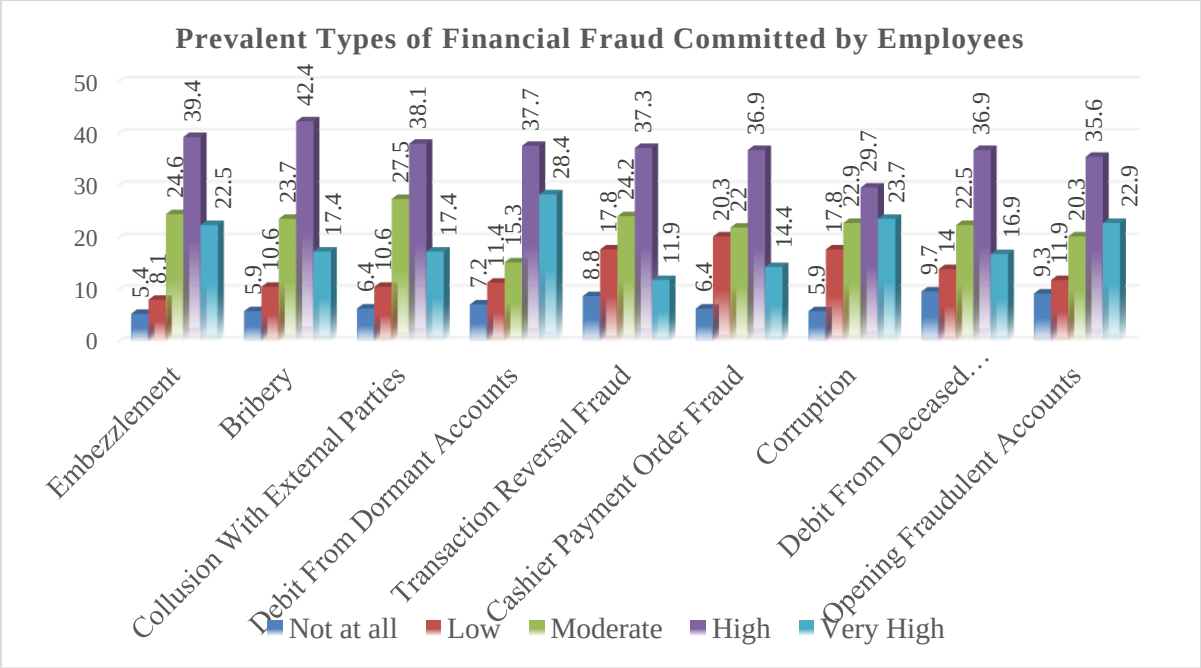
Regarding the statement, "corruption is the prevalent type of financial fraud committed by employees in commercial banks," the survey results show that 29.7 percent of respondents rated it as high, 23.7 percent as very high, 22.9 percent as moderate, 17.8 percent as low, and 5.9 percent as not at all. This statement received a mean score of 3.47 and a standard deviation of 1.201, suggesting a general tendency towards moderate agreement among respondents and a relatively moderate variation in their responses. These types of fraud, often interrelated, undermine institutional integrity and can lead to significant financial losses. Joshi's study supports the notion that internal corruption poses a substantial challenge in financial institutions (Joshi, 2022).

In relation to the statement, "debit from a deceased customer's account is the prevalent type of financial fraud committed by employees in commercial banks," 36.9 percent of respondents rated it as high, 22.5 percent as moderate, 16.9 percent as very high, 14 percent as low, and 9.7 percent as not at all. A total of 76.3 percent of respondents perceive this type of financial fraud to be at least moderately prevalent. This statement received a mean score of 3.37 and a standard deviation of 1.201, indicating a moderate tendency toward higher agreement and a moderate

level of consistency in responses. This finding is supported by the Association of Certified Fraud Examiners, which reports that in Africa and South Asia, deceased account fraud ranks among the top three employee fraud schemes. Bank staff often manipulate dormant account protocols to siphon funds before heirs file claims (ACFE, 2024).

Regarding the statement, "opening fraudulent accounts is the prevalent type of financial fraud committed by employees in commercial banks," 35.6 percent of respondents rated it as high, 22.9 percent as very high, 20.3 percent as moderate, 11.9 percent as low, and 9.3 percent as not at all. A total of 78.8 percent of respondents consider this type of financial fraud to be at least moderately prevalent. This statement received a mean score of 3.51 and a standard deviation of 1.229, reflecting a moderate tendency toward higher agreement and a moderate level of variability in responses. The FFIEC reported that examiners have identified employee-assisted fraudulent account openings as the top fraud risk in U.S. community banks. This issue is linked to incentive-driven sales cultures and weak identity verification practices (FFIEC, 2023).

Figure 4.10: Prevalent Types of Financial Fraud Committed by Employees



Source: Own Survey 2025

When comparing the mean and standard deviation values of various types of financial fraud, Table 4.6 reveals a clear trend in respondents' perceptions of fraud prevalence and the consistency of their responses. "Debit from Dormant Accounts" has the highest mean and a moderate standard deviation, indicating that respondents strongly perceive this type of fraud as prevalent, with little variation in their views. Additionally, "Debit from Dormant Accounts" is considered highly prevalent by respondents, who show a relatively consistent opinion on its significance. In contrast, "Transaction Reversal Fraud," "Cashier Payment Order Fraud," and "Debit from Deceased Customer's Accounts" have the lowest mean values, suggesting that they are regarded as less prevalent types of financial fraud.

Table 4.6: Mean Comparison across Prevalent Types of Financial Fraud Committed by Employees

Comparison across Prevalent Types of Financial Fraud Committed by Employees		
Prevalent Types of Financial Fraud Committed by Employees	Mean	Std. Deviation
Embezzlement	3.65	1.083
Bribery	3.55	1.081
Collusion With External Parties	3.50	1.093
Debit From Dormant Accounts	3.69	1.204
Transaction Reversal Fraud	3.25	1.150
Cashier Payment Order Fraud	3.33	1.141
Corruption	3.47	1.201
Debit From Deceased Customer's Account	3.37	1.201
Opening Fraudulent Accounts	3.51	1.229
Average	3.48	1.154

Source: Own Survey 2025

4.8. Mitigation Strategies

This section presents findings related to preventive measures against financial fraud in commercial banks. The goal of these findings is to provide actionable insights aimed at strengthening the resilience of commercial banks against operational risk and fraudulent

activities, and ensuring the integrity of banking operations. Figure 4.11 below illustrates various preventive measures that should be implemented in commercial banks to mitigate financial fraud. Respondents were asked to share their opinions on the proposed preventive measures using a scale from 1 to 5, where 1 indicates strong disagreement and 5 indicates strong agreement.

Regarding employee training on fraud prevention, the survey revealed that 53.4% of respondents strongly agree with the importance of such training, while 39.8% agree. Only 4.7% chose neutral, 2.1% disagreed, and none selected strongly disagree. A substantial majority, 93.2%, affirmed that regular employee training on fraud prevention is a crucial measure for preventing financial fraud in commercial banks. This statement received a mean score of 4.44, with a standard deviation of 0.685, indicating that most respondents view employee training as a highly effective tool in combating fraud, with low variability in their responses. This finding is supported by ACFE, which states that annual fraud awareness training for employees and managers is one of the most effective preventive controls, reducing fraud occurrence by up to 51% in organizations that implement it (ACFE, 2023).

In terms of implementing advanced real-time fraud detection systems, 55.5% of respondents strongly agree, while 36.9% agree. Only 6.4% chose neutral, 0.8% disagreed, and 0.4% strongly disagreed. A significant majority, 92.4%, believe that investing in advanced fraud detection technology is a critical strategy for enhancing security and minimizing fraud-related losses. This statement received a mean score of 4.46, with a standard deviation of .692, indicating strong agreement among respondents regarding the effectiveness of such systems in reducing fraud risks. This is further supported by the Institute of Internal Auditors (IIA), which recommends that advanced fraud detection technologies, including real-time monitoring and artificial intelligence, should be implemented as preventive controls to mitigate operational risks and reduce exposure to financial fraud (IIA, 2015).

Regarding the strengthening of internal controls, 64.4 percent of respondents strongly agreed, 33.1 percent agreed, 1.7 percent remained neutral, 0.8 percent disagreed, and none strongly disagreed. Almost all respondents (97.5%) recognized the importance of strengthening internal controls as a crucial measure to prevent financial fraud in commercial banks. This statement received a mean score of 4.61, with a standard deviation of .569, reflecting a consensus on the

critical role that well-structured and effective internal control mechanisms play in fraud prevention. The IIA emphasizes that effective internal controls are foundational for fraud prevention and operational risk management. Organizations must continuously assess and enhance these controls to address evolving risks (IIA, 2023).

In terms of collaboration between banks and regulators, 46.6 percent of respondents agreed, 43.6 percent strongly agreed, 8.5 percent were neutral, 1.3 percent disagreed, and none strongly disagreed. A significant proportion of respondents (90.2%) acknowledged collaboration between banks and regulators as a vital measure to prevent financial fraud. This statement received a mean score of 4.33 and a standard deviation of .684, indicating a shared agreement on the effectiveness of this collaboration, with low variability in responses. The BCBS asserts that close cooperation between banks and supervisory authorities is essential for identifying emerging risks and preventing systemic fraud. Supervisors should maintain open dialogue with banks to strengthen controls and enhance early warning systems (BCBS, 2012)

Regarding enhanced employee screening during recruitment, 44.1 percent of respondents agreed, 41.5 percent strongly agreed, 12.3 percent remained neutral, 1.7 percent disagreed, and 0.4 percent strongly disagreed. A substantial majority (85.6%) identified enhanced employee screening during recruitment as a key preventive measure for mitigating operational risk and preventing financial fraud. This measure received a mean score of 4.25, with a standard deviation of .766, indicating a high level of agreement along with some variability in recognizing rigorous recruitment processes as essential for ensuring that only qualified and trustworthy individuals are hired. This aligns with the Basel Committee on Banking Supervision report, which states that enhanced due diligence in hiring, including criminal record checks and credential verification, is a critical preventive control to mitigate insider risk in financial institutions (BCBS, 2021).

In a survey regarding customer awareness programs on fraud prevention, 49.2% of respondents agreed that these programs are effective, while 37.7% strongly agreed. Additionally, 11.9% remained neutral, 0.8% disagreed, and 0.4% strongly disagreed. A significant majority of respondents (86.9%) recognized customer awareness programs on fraud prevention as essential measures for mitigating operational risks and preventing financial fraud. This viewpoint received a mean score of 4.29, with a standard deviation of .719, indicating a broad

consensus on the importance of informed customers in detecting fraudulent activities and protecting themselves. According to ACFE's report, organizations that implement regular customer fraud awareness programs can reduce fraud losses by as much as 35%, as educated customers are less likely to become victims of social engineering scams (ACFE, 2024).

To strengthen the fraud investigation process, the survey results showed that 47.9% of respondents agreed, 44.5% strongly agreed, 5.5% were neutral, and 2.1% disagreed, with no respondents selecting 'strongly disagree.' A significant majority, 92.4%, acknowledged that enhancing the fraud investigation process is a crucial preventive measure against financial fraud. This viewpoint received a mean score of 4.35, indicating a strong recognition of the importance of improving procedures for detecting, investigating, and resolving financial fraudulent activities. The IIA emphasizes that effective fraud investigation processes, which include documented procedures and trained personnel, are essential for deterring future fraud and minimizing operational disruptions (IIA, 2023).

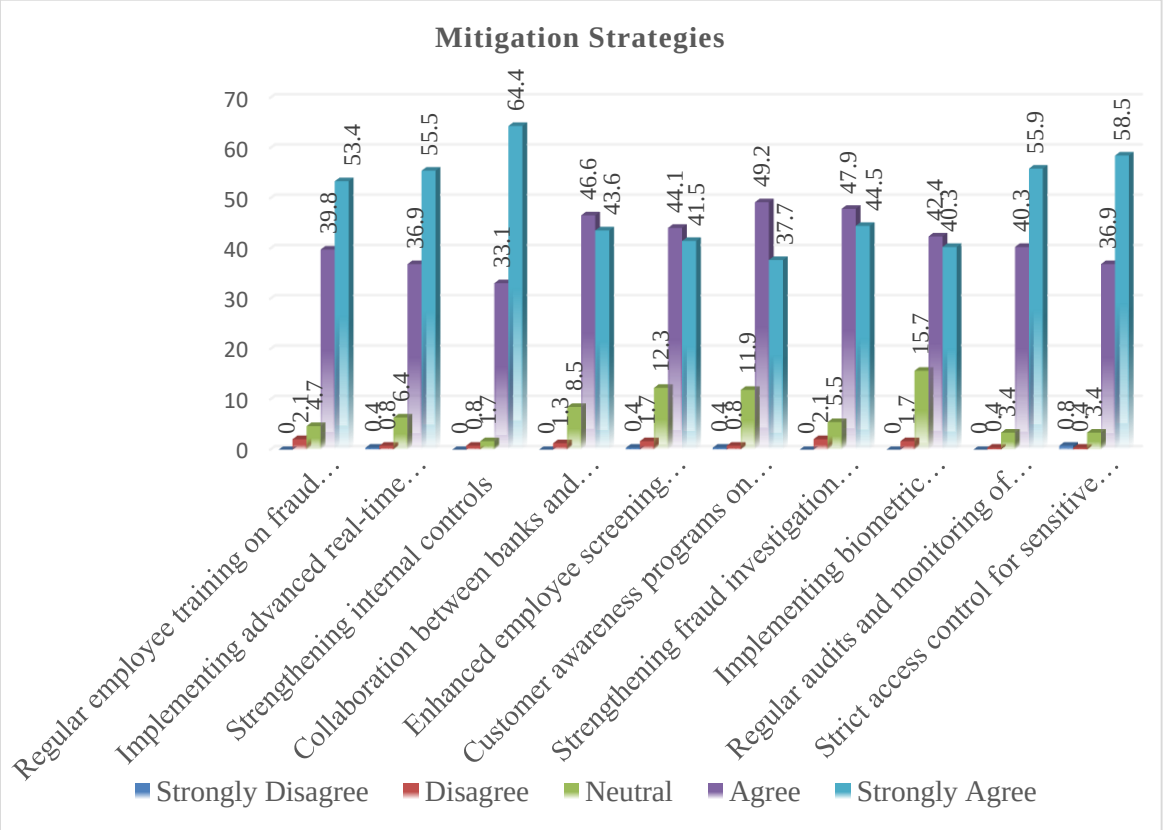
Concerning the implementation of biometric authentication systems, 42.4% of respondents agreed, 40.3% strongly agreed, 15.7% were neutral, and 1.7% disagreed, with no participants choosing 'strongly disagree.' A significant 82.7% of respondents indicated that implementing biometric authentication systems is a valuable preventive measure against operational risk and financial fraud. This statement received a mean score of 4.21, demonstrating a widespread recognition of the potential for biometrics to enhance security and prevent unauthorized access to the banking system. The FFIEC recommends that biometric authentication methods (such as fingerprint and facial recognition) provide a higher level of assurance than traditional credentials and should be implemented as part of a layered security approach to mitigate fraud risks (FFIEC, 2021).

Regarding the topic of regular audits and monitoring of high-risk accounts, 55.9% of respondents strongly agreed, while 40.3% agreed, 3.4% remained neutral, and 0.4% disagreed. Notably, there were no responses for "strongly disagree." A significant majority, 96.2%, acknowledged that regular audits and monitoring of high-risk accounts are essential preventive measures against operational risk and financial fraud. This statement received a mean score of 4.52, accompanied by a standard deviation of .587, highlighting the importance of implementing robust mechanisms for these practices, with consistent agreement among

respondents. The BCBS recommends that institutions conduct continuous monitoring and periodic audits of high-risk accounts to identify anomalies and prevent fraudulent activities (BCBS, 2021).

In terms of strict access control for sensitive systems, 58.5% of respondents strongly agreed, 36.9% agreed, 3.4% were neutral, 0.8% strongly disagreed, and 0.4% disagreed. A substantial portion, 95.4%, considered that enforcing strict access controls for sensitive systems is a critical preventive measure against operational risk and financial fraud. This statement achieved a mean score of 4.52 and a standard deviation of .668, emphasizing the important role of strict access controls as a cornerstone for securing transactions and mitigating fraud risks. The FFIEC advises financial institutions to implement strict access controls (such as multi-factor authentication and segregation of duties) for high-risk systems (including payment processing and customer databases) to avert fraud (FFIEC, 2023).

Figure 4.11: ***Mitigation Strategies***



Source: Own Survey 2025

As demonstrated in Table 4.7, strengthening internal controls received the highest mean score of 4.61, indicating strong agreement among respondents about its importance as a key factor. Additionally, it has the lowest standard deviation of 0.569, reflecting a high level of consensus. In contrast, implementing biometric authentication systems has the lowest mean score of 4.21 and exhibits the greatest variability among responses, with a standard deviation of 0.765.

Table 4.7: Mean Comparison across Mitigation Strategies

Mean Comparison across Mitigation Strategies		
Mitigation Strategies	Mean	Std. Deviation
Regular employee training on fraud prevention	4.44	0.685
Implementing advanced real-time fraud detection systems	4.46	0.692
Strengthening internal controls	4.61	0.569
Collaboration between banks and regulators	4.33	0.684
Enhanced employee screening during recruitment	4.25	0.766
Customer awareness programs on fraud prevention	4.23	0.719
Strengthening fraud investigation processes	4.35	0.683
Implementing biometric authentication systems	4.21	0.765
Regular audits and monitoring of high-risk accounts	4.52	0.587
Strict access control for sensitive systems	4.52	0.668
Average	4.39	0.682

Source: Own Survey 2025

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATION

5.1 Introduction

This chapter offers a clear summary of the research findings, conclusions drawn from the analysis, and recommendations based on the study's outcomes. It reviews the key points discussed in the previous chapter, highlighting significant findings related to the factors contributing to operational risk and financial fraud from both internal and external perspectives. Internally, the chapter examines the processes and systems, human factors, and employees involved. Externally, it addresses factors related to customers and the broader environment. The chapter outlines the essential components of operational risk and the common types of financial fraud perpetrated by both employees and customers. Additionally, it discusses preventive measures and mitigation strategies that can be implemented. The conclusion summarizes the findings in relation to the research objectives, providing an interpretation of their implications. The recommendations present actionable insights and strategies aimed at reducing operational risk and preventing financial fraud. By integrating the study's results with practical applications, this chapter aims to enhance both academic understanding and operational improvements within the banking sector.

5.2 Summary

This study aimed to explore the factors contributing to operational risk in commercial banks, the prevalent types of financial fraud, and mitigation strategies. A descriptive research approach was employed, with data collected through questionnaires distributed to internal audit, internal control, risk management, compliance, and ethics and anti-corruption departments across all 31 commercial banks. The research identified key internal process and systems factors that contribute to operational risk. These include inadequate IT systems and infrastructure, weak transaction authentication protocols, lack of segregation of duties, poor documentation practices, and insufficient real-time monitoring systems. Human factors also played a significant role, such as a weak ethical culture within the organization, a lack of accountability and oversight, a lack of employee training, insufficient background checks during hiring, and employee misconduct. External factors were identified that include cyber security threats, political and economic instability, lack of specialized oversight for emerging technologies, weak enforcement of compliance standards, and inconsistent enforcement of

anti-fraud regulations. The study documented prevalent types of fraud committed by customers, such as mobile banking fraud, cheque fraud, money laundering, and identity theft, which were identified as the most common. Among employees, the most prevalent types of fraud included debits from dormant accounts, embezzlement, bribery, and collusion with external parties. Additionally, the findings highlighted critical measures for mitigating operational risk and preventing fraud, such as strengthening internal controls, conducting regular audits and monitoring of high-risk accounts, implementing strict access control for sensitive systems, implementing advanced real-time fraud detection systems, and providing regular employee training on fraud prevention. These insights emphasize the importance of a multifaceted approach to mitigate operational risk and prevent financial fraud in the banking sector.

5.3 Conclusion

This study confirms that operational risk in Ethiopian commercial banks stems from three primary sources:

1. Internal Process and System Weaknesses
2. Human Factor Vulnerabilities
3. External Environmental Pressures

The research systematically addresses each of its stated objectives, yielding the following key findings:

Key Findings by Research Objective

1. Assessment of Internal Processes & Systems
    - Critical Deficiencies Identified:
        - Inadequate IT systems and infrastructure
        - Inadequate transaction authentication protocols
        - Poor segregation of duties and documentation practices
        - Lack of real-time monitoring capabilities
2. Evaluation of Human Factors

- Significant Risk Contributors:
    - Weak organizational ethical culture
    - Insufficient accountability mechanisms
    - Inadequate employee training programs
    - Lax background checks during recruitment
    - Prevalence of employee misconduct

3. Analysis of External Risk Factors
    - Major External Threats:
        - Increasing cybersecurity risks
        - Political and economic instability
        - Regulatory gaps in emerging technologies
        - Inconsistent enforcement of compliance standards
        - Weak anti-fraud regulation implementation
4. Identification of Prevalent Fraud Types
    - Customer-Perpetrated Fraud:
        - Mobile banking fraud
        - Cheque fraud
        - Money laundering
        - Identity theft
    - Employee-Perpetrated Fraud:
        - Unauthorized debits from dormant accounts
        - Embezzlement
        - Bribery
        - Collusion with external parties

5. Proposed Mitigation Strategies
    - Key Recommendations:
        - Strengthening internal control frameworks
        - Implementing rigorous audit procedures for high-risk accounts
        - Enforcing strict access controls on sensitive systems
        - Deploying AI-powered, real-time fraud detection systems
        - Conducting regular, comprehensive employee training programs

5.4 Recommendations

Based on the findings of this study, the following recommendations are made to mitigate operational risk, prevent financial fraud, and strengthen fraud prevention mechanisms in commercial banks:

For Commercial Banks:

1. IT Infrastructure Modernization
    - Prioritize upgrading core banking systems with biometric authentication (fingerprint/facial recognition) for high-risk transactions, as our study found weak authentication protocols contribute to 88.2% of fraud cases.
    - Implement AI-powered real-time monitoring systems specifically targeting dormant account activities, given that debit from dormant accounts was identified as the most prevalent employee fraud (mean score 3.69).
2. Human Resource Controls
    - Establish mandatory quarterly fraud awareness training with case studies from recent Ethiopian banking fraud incidents (March 2024 CBE incident), as 91.5% of respondents linked training gaps to operational risk.
    - Implement forensic accounting techniques during employee screening, particularly for roles in internal audit and risk management departments which comprised 71.2% of our respondents.
3. Process Optimization

- Automate reconciliation processes for high-volume transactions like mobile banking (78.4% prevalence) and cheque processing (66.1% prevalence), which our data shows are particularly vulnerable.
- Develop specialized fintech oversight teams to monitor emerging technologies like blockchain-based transactions, as 88.2% of experts cited this as a critical gap.

For Regulatory Bodies (National Bank of Ethiopia):

1. Regulatory Framework Updates
    - Create a dedicated cybersecurity regulatory unit focusing on mobile banking fraud prevention, as this fraud type showed the highest prevalence (mean 4.06) among customer-perpetrated frauds.
    - Implement mandatory fraud reporting standards with specific timelines, as inconsistent enforcement was identified by 85.2% of respondents as increasing fraud risks.
2. Capacity Building
    - Develop specialized training programs for bank examiners on investigating employee collusion cases, which accounted for 83% of high-loss fraud incidents according to our findings.
    - Establish a central fraud database incorporating patterns from all 31 commercial banks to enable predictive analytics.

For Future Research:

1. Technology-Focused Studies
    - Conduct action research on implementing Ethiopia-specific AI models for detecting the top 3 fraud types identified: mobile banking fraud, cheque fraud, and dormant account fraud.
    - Investigate the behavioral economics behind employee rationalization of fraud in Ethiopian cultural context, as our data showed 83.9% recognition of employee misconduct as significant.

2. Sector-Specific Investigations

- Perform comparative studies between large (CBE), medium (5 banks), and small (25 banks) banks regarding fraud vulnerability, as our study encompassed all categories but identified differing risk profiles.
- Examine the gender dimensions of fraud perpetration and prevention, given the 4.6:1 male-to-female ratio in banking sector positions identified in our demographic analysis.

References

Abebe, T., 2015. Regulatory Compliance and Operational Risk Management in Ethiopian Commercial Banks. *Ethiopian Journal of Business and Economics,* 5(2), pp. 45-67.

Addis Fortune, 2022. *Ethiopian Banks Lose Billions to Fraud.* [Online]
Available at: https://addisfortune.net
[Accessed 15 April 2025].

Addis Fortune, 2024. *System Malfunction at Commercial Bank of Ethiopia.* [Online]
Available at: https://addisfortune.net
[Accessed 15 April 2025].

Adekunle, I. & Adetiloye, K., 2013. Operational Risk Management and Regulatory Challenges in African Banking Sectors. *African Journal of Economic and Management Studies,* 4(2), pp. 178-195.

Adeoye, A. & Rahman, M., 2020. Dormant Account Fraud in Commercial Banks: A Silent Epidemic. *Journal of Financial Crime,* 27(3), pp. 789-805.

Adeyemi, K., 2011. Bank Failure in Nigeria: Consequences of Capital Inadequacy, Poor Asset Quality and Ineffective Monitoring. *African Journal of Accounting, Economics, Finance and Banking Research,* 7(7), pp. 27-44.

Afjal, M., Salamzadeh, A. & Dana, L., 2023. Financial fraud and credit risk: Illicit practices and their impact on banking stability. *Journal of Risk and Financial Management,* 16(9), p. 386.

Akers, R. L., 1996. *Social Learning and Social Structure: A General Theory of Crime and Deviance.* Boston: Northeastern University Press.

Akers, R. L. & Gissel, J. D., 2006. Fraud triangle: Opportunity knocks. ,. *Journal of Accountancy,* 201(6), pp. 63-67.

Albrecht, W., Howe, K. & Romney, M., 1984. *Fraud: The Unmanaged Risk.* Cambridge: MIT Press.

Alexander, C., 2003. Managing Operational Risks from External Shocks: The Role of Business Continuity Planning. *Journal of Financial Regulation and Compliance,* 11(3), pp. 210-225.

Allen, L. & Bali, T., 2007. Cyclicality in Catastrophic and Operational Risk Measurements. *Journal of Banking & Finance,* 31(4), pp. 1191-1235.

Aragie, A., 2011. *Fraud In Ethiopian Banks: Causes and Prevention.* Addis Ababa: Addis Ababa University.

Association of Certified Fraud Examiners, 2020. *Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse,* Austin: Association of Certified Fraud Examiners.

Association of Certified Fraud Examiners, 2022. *Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse,* Austin: ACFE.

Association of Certified Fraud Examiners, 2023. *Fraud 101: What is fraud?,* Austin: Association of Certified Fraud Examiners.

Association of Certified Fraud Examiners, 2024. *Report to the Nations: 2024 Global Study on Occupational Fraud and Abuse,* Austin: ACFE.

Bangladesh Bank, 2023. *Annual Report on Banking Frauds & Forgeries,* Dhaka: Bangladesh Bank.

Basel Committee on Banking Supervision, 2001. *Operational Risk,* Basel: Bank for International Settlements.

Basel Committee on Banking Supervision, 2011. *Operational Risk - Supervisory Guidelines for the Advanced Measurement Approaches,* Basel: Bank for International Settlements.

Basel Committee on Banking Supervision, 2011. *Principles for the Sound Management of Operational Risk,* Basel: Bank for International Settlements.

Basel Committee on Banking Supervision, 2012. *Core Principles for Effective Banking Supervision,* Basel: Bank for International Settlements.

Basel Committee on Banking Supervision, 2021. *Principles for the Sound Management of Operational Risk,* Basel: Bank for International Settlements.

Basel Committee on Banking Supervision, 2023. *Digital Fraud and Banking: Supervisory and Financial Stability Implications,* Basel: Bank for International Settlements.

Bhasin, M., 2015. Combating Financial Fraud: A Case Study on The Banking Sector. *The International Journal of Business and Management Research,* 3(2), pp. 45-60.

Bhasin, M., 2016. Fraud Prevention in the Banking Industry: Challenges and Strategies. *Journal Of Financial Crime,* 23(4), pp. 934-950.

Bhasin, M., 2016. Internal Corruption in Financial Institutions: A study of Employee Collusion. *Journal of Financial Crime,* 29(3), pp. 450-467.

Bhattacherjee, A., 2012. *Social Science Research: Principles, Methods, and Practices.* 2nd ed. Tampa: University of South Florida.

Birhanu, T., 2025. *Operational Risk and Financial Fraud in Ethiopian Banks.* Addis Ababa: Addis Ababa University.

Birhanu, Y., 2025. *Why Financial Fraud in Ethiopia? A Case Study on Selected Commercial Banks.* Addis Ababa: Addis Ababa University.

Bryman, A. & Bell, E., 2011. *Business Research Methods.* 3rd ed. Oxford: Oxford University Press.

Bryman, A. & Bell, E., 2011. *Business Research Methods.* 3rd ed. Oxford: Oxford University Press.

Chapelle, A., Crama, Y., Hübner, G. & Peters, J. P., 2008. Practical methods for measuring and managing operational risk in the financial sector: A clinical study. *Journal of Banking & Finance,* 32(6), pp. 1049-1061.

Chelangat, L., 2014. Embezzlement Risks in Fnancial Institutions: The Role of Internal Controls. *Journal of Financial Regulation and Compliance,* 22(3), pp. 245-260.

Chen, J., 2024. *What is money laundering?,* New York: Investopedia.

Chernobai, A. M. C. R. S. a. T. S., 2007. Empirical Analysis of Operational Risk Factors in the Banking Industry. *Journal of Operational Risk,* 2(4), pp. 1-27.

Cope, E. & Labbi, A., 2012. Operational Risk and Financial Fraud: Evidence from Banking Loss Data. *Journal of Operational Risk,* 7(4), pp. 3-24.

Cope, E. & Labbi, A., 2012. Operational Risk and Financial Fraud: Evidence from Banking Loss Data. *Journal of Operational Risk,* 7(4), pp. 3-24.

Council, F. F. I. E., 2022. *Supervisory Highlights: Fraud in Banking Operations,* Washington, DC: Federal Financial Institutions Examination Council.

Cressey, D., 1973. *Other People's Money: A Study in the Social Psychology of Embezzlement.* New York: Free Press.

Creswell, J., 2009. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* 3rd ed. Sage Publications: Thousand Oaks.

Cruz, M. G., 2002. *Modeling, Measuring and Hedging Operational Risk.* Hoboken, New Jersey, Wiley Finance.

Deloitte, 2023. *Payment Fraud Trends in Banking,* London: Deloitte Touche Tohmatsu.

Dennis, S., Osei, K. & Mensah, J., 2018. Employee Fraud in Ghanaian Banks: The Role of Corporate Culture and Internal Control Failures. *Journal of Financial Crime,* 25(3), pp. 825-843.

Elliott, R. K. & Willingham, J. J., 1980. *Management Fraud: Detection and Deterrence.* New York: Petrocelli Books.

Ethics & Compliance Initiative, 2023. *Global Business Ethics Survey,* Arlington: ECI.

Examiners, A. o. C. F., 2023. *Report to the Nations: Occupational Fraud and Abuse,* Austin: Association of Certified Fraud Examiners.

Federal Financial Institutions Examination Council, 2021. *Authentication and Access to Financial Institution Services and Systems,* Washington, DC: FFIEC.

Federal Financial Institutions Examination Council, 2022. *Supervisory Highlights: Fraud in Banking Operations,* Washington, DC: FFIEC.

Federal Financial Institutions Examination Council, 2023. *IT Examination Handbook,* Washington, DC: FFIEC.

Financial Action Task Force, 2022. *Money Laundering and Terrorist Financing Risks in Commercial Banks,* Paris: FATF.

Financial Action Task Force, 2022. *Money Laundering Vulnerabilities in Commercial Banking,* Paris: FATF.

Financial Action Task Force, 2023. *Terrorist Financing Risks in High-Risk Jurisdictions,* Paris: FATF.

Fraser, J. & Simkins, B. J. (., 2016. *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives.* Hoboken, New Jersey: Wiley.

Gashayie, A. & Singh, M., 2016. Banking Sector Development in Ethiopia: Challenges and Opportunities. *International Journal of Economics and Finance,* 8(5), pp. 123-135.

Gebremichael, A., 2017. Human Capital Investment and Operational Risk Mitigation in Ethiopian Commercial Banks. *Ethiopian Journal of Business and Economics,* 6(1), pp. 78-102.

Gebreselasie, T., 2022. *Cheque Fraud in Ethiopian Commercial Banks.* Addis Ababa: Addis Ababa University Press.

Gebreselasie, T., 2022. *Fraud Prevention and Detection in Ethiopian Commercial Banks.* Addis Ababa: Addis Ababa University.

Geffner, M., 2014. Multilayered Defenses against Evolving Fraud Schemes in Digital Banking. *Journal of Cybersecurity and Financial Protection*, 6(2), pp. 45-62.

George, D. & Mallery, P., 2010. *SPSS for Windows Step by Step: A Simple Guide and Reference, 17.0 Update.* 10th ed. Boston: Pearson.

George, D. & Mallery, P., 2019. *IBM SPSS Statistics 26 Step by Step: A Simple Guide and Reference.* 16th ed. New York: Routledge.

Getachew, A., 2021. Effectiveness of Internal Control Systems in Fraud Prevention: Evidence from Ethiopian Commercial Bank. *African Journal of Accounting and Auditing Research*, 8(1), pp. 45-68.

Greenbaum, S. I. & Thakor, A. V., 2007. *Contemporary financial intermediation.* 2nd ed. Burlington, MA: Academic Press.

Harris, L., 2024. *Fraud Detection in the Financial Sector Using Advanced Data Analysis Techniques.* Stanford: Stanford University.

Hoffman, D., 2002. *Managing Operational Risk in Financial Institutions: The Role of Internal Controls.* Chicago: Banking Risk Publications.

Hollinger, R. C. & Clark, J. P., 1983. *Theft by employees.* Lexington: Lexington Books.

Hopkin, P., 2018. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management (5th ed.). Kogan Page.*. 5th ed. London: Kogan Page.

IBM, 2022. *Breaking Barriers: How Communication Drives Performance,* Armonk, NY: IBM Corporation.

Institute of Internal Auditors, 2009. *GTAG 8: Auditing Fraud Risks,* Altamonte Springs, FL: The Institute of Internal Auditors.

Institute of Internal Auditors, 2015. *GTAG 17: Auditing IT Governance,* Lake Mary, FL: IIA.

Institute of Internal Auditors, 2023. *International Professional Practices Framework (IPPF),* Lake Mary, FL: IIA.

International Auditing and Assurance Standards Board, 2022. *International Standard on Auditing (ISA) 240: The auditor's responsibilities relating to fraud in an audit of financial statements,* New York: International Federation of Accountants (IFAC).

International Organization for Standardization, 2021. *ISO 37301:2021 Compliance Management Systems - Guidelines.* Geneva: ISO.

Joshi, A., 2022. Internal Corruption in Financial Institutions: A Study of Employee Collusion. *Journal Of Financial Crime,* 29(3), pp. 450-467.

Kothari, C., 2004. *Research Methodology: Methods and Techniques.* 2nd ed. New Delhi: New Age International Publishers.

Lam, J., 2014. *Enterprise Risk Management: From Incentives to Controls.* 2nd ed. Hoboken, New Jersey: Wiley.

McKinsey & Company, 2022. *The Great Attrition and Operational Resilience,* New York: Mckinsey & Company.

Mishkin, F. S., 2006. *The Economics of Money, Banking, and Financial Markets.* 8th ed. Boston: Pearson.

Mueller, J., 2015. *Fraud Detection and Prevention in the Digital Age: How Analytics is Transforming Financial Security.* New York: Wiley.

Mulugeta, D., 2018. Process Inefficiencies and Operational Rsk in Ethiopian Banking: The Case for Procedural Standardization. *Journal of African Business,* 19(2), pp. 234-256.

National Bank of Ethiopia, 2023. *Annual Report 2022/23,* Addis Ababa: NBE.

National Bank of Ethiopia, 2024. *Financial Stability Report,* Addis Ababa: NBE.

Omar, N. & Din, M. M., 2010. The Role of Social Engineering in Enabling Financial raud: A Malaysian Perspective. *Journal of Financial Crime,* 17(4), pp. 407-420.

Onkagba, S. O., 1993. Patterns of Bank Fraud in Nigeria: The Account Opening Scheme.. *Journal of Financial Crime,* 1(2), pp. 147-155.

Owojori, A., Akintoye, I. & Adidu, F., 2011. The Challenge of Risk Management in Nigerian Banks. *International Journal of Business and Management,* 6(3), pp. 198-212.

Power, M., 2007. *Organized Uncertainty: Designing a World of Risk Management.* Oxford: Oxford University Press.

Power, M., 2013. The Risk Management of Everything. *Journal of Risk Finance,* 14(3), pp. 267-274.

Power, M., 2013. The Risk Management of Everything.. *Journal of Risk Finance,* 14(3), pp. 267-274.

Quah, J. & Sriganesh, M., 2008. Real-time Credit Card Fraud Detection using Computational Intelligence. *Expert Systems with Applications,* 35(4), pp. 1721-1732.

Quah, J. & Sriganesh, M., 2008. Real-Time Credit Card Fraud Detection Using Computational Intelligence. *Expert Systems with Applications,* 35(4), pp. 1721-1732.

Sanusi, N., Ismail, S. & Abidin, S., 2015. Fraud Typologies in Malaysian Banking: An Empirical Analysis of Detection and Prevention. *Journal of Financial Crime,* 22(2), pp. 178-195.

Sanusi, Z., Rameli, M. & Isa, Y., 2015. Fraud in the Nigerian Banking Sector: A Review of Cases. *Journal of Financial Crime,* 22(2), pp. 234-248.

Segal, T., 2024. New York: Investopedia.

Setarge, K., 2022. *Digital Banking Security Challenges in Ethiopia.* Addis Ababa: Ethiopian Banking Institute.

Setarge, T., 2022. Fraud Detection and Prevention in Ethiopian Commercial Banks. *Journal of Risk and Financial Management,* 15(4), pp. 156-170.

Silverstone, H. & Davia, H. R., 2005. *Fraud 101: Techniques and Strategies for Detection.* 3rd ed. Hoboken, New Jersey: Wiley.

Sutherland, E. H., 1949. *White collar crime.* New York: Dryden Press.

Tadesse, S., 2016. IT Infrastructure Challenges and Operational Risk in Ethiopian Banks: The Case for Strategic Investment. *African Journal of Information Systems,* 8(3), pp. 22-41.

U.S. Government Accountability Office, 2023. *Cybersecurity: High-Risk Series,* Washington, DC: GAO.

U.S. Government Accountability Office, 2023. *Emerging Technologies: Additional Federal Guidance could Improve Oversight,* Washington, DC: GAO.

Wanjohi, M., 2014. *Fraud in the Banking Industry in Kenya: A Case of Commercial Bank of Africa, Kenya.* Nairobi: United States International University Africa.

Weis, T., Rawlins, M., Itana, K. & Coleman, R., 2022. *The Leadership Gender Gap in Banking: Insights from Ethiopia,* Washington, DC: World Bank.

Wells, J., 2017. *Corporate Fraud Handbook: Prevention and Detection.* 5th ed. Hoboken, NJ: John Wiley & Sons.

Wells, J. T., 2013. *Principles of fraud examination.* 4th ed. Hoboken, New Jersey: Wiley.

Wendels, R., Bennett, R. & Cressy, R., 2009. The Detection and Prevention of External Fraud in Retail Banking. *Journal of Financial Crime,* 16(3), pp. 223-241.

Wolfe, D. & Hermanson, D., 2004. The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal,* 74(12), pp. 38-42.

Wolfe, D. T. & Hermanson, D. R., 2004. The Fraud Diamond: Considering the Four Elements of Fraud.. *CPA Journal,* 74(12), pp. 38-42.

Worku, F., 2018. *The Impact of Internal Control Systems on Fraud Prevention in Ethiopian Banks.* Addis Ababa: Addis Ababa University.

Worku, G., 2020. *Phishing Scams in Ethiopian Financial Institutions.* Addis Ababa: Ethiopian Cyber Security Agency.

Worku, Y., 2020. *E-Banking Fraud in Ethiopia: Causes and Management Practices.* Addis Ababa: Addis Ababa University.

World Bank, 2016. *Bank Fraud: The Case of Employee Embezzlement,* Washington, DC: World Bank Group.

World Bank, 2019. *Diagnosing Corruption in Financial Services: A Risk-based Approach.,* Washington, DC: World Bank Group.

World Bank, 2020. *Enhancing Financial Regulation to Prevent Fraud,* Washington, DC: World Bank.

World Bank, 2022. *Global Economic Prospects: Navigating Political Instability,* Washington, DC: World Bank Group.

Yalew, T., 2021. *Effects of Fraud on Bank Performance in Ethiopian Commercial Banks..* Addis Ababa: Addis Ababa University .

Zahra, S., Priem, R. & Rasheed, A., 2007. Understanding the Causes and Effects of Corporate Fraud. *Business Horizons,* 50(6), pp. 477-488.

Addis Ababa University

College of Business and Economics

School of Commerce

Questionnaire to be collected from Staff Commercial Banks in Ethiopia

Informed Consent

My name is Zemichael Tesfamariam, MSC student at Addis Ababa University School of Commerce. Currently, I am working on my thesis entitled "**Operational Risk in Ethiopian Commercial Banks: A Case Study with Emphasis on Financial Fraud".** I am conducting this study as a partial fulfillment of the requirements of the Master of Science degree in Corporate Finance specialty in Investment Management. Thus, this questionnaire is prepared to collect data for you as representatives of the banks. Accordingly, the study has identified you as a vital source of primary data which is very compulsory to complete the study appropriately. Hence, the responses you provide in this questionnaire are very pertinent in that they enable the researcher to come up with valid, credible, and valuable research findings. Such findings, in turn, are very crucial in that they enable the creation of improved understanding among stakeholders regarding **Operational Risk in Ethiopian Commercial Banks: A Case Study with Emphasis on Financial Fraud.** The true responses you give will thus be used as pertinent primary information for the study and have a large contribution to the achievement of the thesis.

The purpose of the study is exclusively academic. Hence, the personal identity of respondents will be kept anonymous in all processes of the study and therefore, no one knows who has participated in responding to this questionnaire. Besides, the information you may provide in this questionnaire will be held confidential and it is exclusively used for doing this research. Hence, I kindly request you to be honest and benevolent in providing the right answers to the questionnaire. It will take you about 20 minutes to have answers to the questions listed in the questionnaire. Therefore, I kindly ask you to have patience in answering the questions well. I am very grateful for your support in advance!

Zemichael Tesfamariam

Appendix 1: Questionnaire

Section I: Demographic Information

This section collects basic information about the respondents to ensure a diverse and representative sample.

1. **Age**:
    - 18-25 ☐
    - 26-35 ☐
    - 36-45 ☐
    - 46-55 ☐
    - Above 55 ☐
2. **Gender**:
    - Male ☐
    - Female ☐
3. **Educational Background**:
    - Diploma ☐
    - BA Degree ☐
    - Masters ☐
    - PhD & Above ☐
4. **Department**:
    - Internal Audit ☐
    - Internal Control ☐
    - Risk Management ☐
    - Compliance ☐
    - Ethics and Anti-Corruption ☐
    - Other (Please specify): _____
5. **Work Experience**:
    - <1 Year ☐
    - 1 to 5 Years ☐
    - 6 to 10 Years ☐
    - 10 Years ☐

Section II: Internal Processes and Systems

This section assesses the sources of internal processes and systems contributing to operational risk.

6. **What are your views on the following statements regarding internal processes and systems?***(Please use a scale of 1 to 5, where 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)*

S. No	Statement	1	2	3	4	5
1	Lack of segregation of duties increases operational risk and fraud.					
2	Poor documentation practices contribute to operational inefficiencies.					
3	Weak transaction authentication protocols increase fraud risks.					
4	Inadequate IT systems and infrastructure increase operational risks.					
5	Manual processes are a significant source of operational risk.					
6	Lack of real-time monitoring systems increases fraud risks.					
7	Poor interdepartmental communication leads to operational inefficiencies					
8	Limited process automation increases operational risks					

Section III: Human Factors

This section evaluates the role of human factors (e.g., employee behavior, training) in operational risk.

7. What are your views on the following statements regarding human factors?
(Please use a scale of 1 to 5, where 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

S. No	Statement	1	2	3	4	5
1	Lack of employee training increases operational risk and fraud.					
2	High employee turnover rates contribute to operational inefficiencies.					
3	Employee misconduct is a significant source of financial fraud.					
4	Insufficient background checks during hiring increase fraud risks.					
5	Pressure to meet financial targets leads to fraudulent activities.					
6	Lack of accountability and oversight increases operational risks.					
7	Weak ethical culture within the organization encourages misconduct					
8	Inadequate incentive structures represent a measurable fraud risk factor within organizations					

Section IV: External Factors

This section analyzes the influence of external factors (e.g., regulatory environment, technological infrastructure) on operational risk.

8. **What are your views on the following statements regarding external factors?**
   (Please use a scale of 1 to 5, where 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

S. No	Statement	1	2	3	4	5
1	Weak enforcement of compliance standards increases operational risks.					
2	Outdated regulatory frameworks contribute to financial fraud.					
3	Lack of specialized oversight for emerging technologies increases risks.					
4	Inconsistent enforcement of anti-fraud regulations increases fraud risks.					
5	Regulatory bodies lack sufficient resources to combat fraud effectively.					
6	Political and economic instability exacerbate operational risks.					
7	Cyber security threats (e.g., hacking) pose significant operational risks					
8	Fraud risks are amplified due to inadequate third-party vendor risk management					

Section V: Types of Financial Fraud

This section identifies the prevalent types of financial fraud committed by customers and employees.

9. **What are your views on the following types of financial fraud committed by customers?**
   (Please use a scale of 1 to 4, where 1 = Not at all, 2 = Low, 3 = Moderate, 4 = High, 5 = Very High)

S. No	Type of Fraud	1	2	3	4	5
1	Identity Theft					
2	Cheque Fraud					
3	Debit Card Fraud					
4	Mobile Banking Fraud					
5	Phishing Scams					
6	Money Laundering					
7	Terrorist Financing					

10. **What are your views on the following types of financial fraud committed by employees?**
(Please use a scale of 1 to 4, where 1 = Not at all, 2 = Low, 3 = Moderate, 4 = High, 5 = Very High)

S. No	Type of Fraud	1	2	3	4	5
1	Embezzlement					
2	Bribery					
3	Collusion With External Parties					
4	Debit From Dormant Accounts					
5	Transaction Reversal Fraud					
6	Cashier Payment Order Fraud					
7	Corruption					
8	Debit From Deceased Customer's Account					
9	Opening Fraudulent Accounts					

Section VI: Mitigation Strategies

11. This section proposes strategies for mitigating operational risk and preventing financial fraud.

What are your views on the following preventive measures?
(Please use a scale of 1 to 5, where 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, Neutral, 4 = Agree, 5 = Strongly Agree)

S. No	Preventive Measure	1	2	3	4	5
1	Regular employee training on fraud prevention					
2	Implementing advanced real-time fraud detection systems					
3	Strengthening internal controls					
4	Collaboration between banks and regulators					
5	Enhanced employee screening during recruitment					
6	Customer awareness programs on fraud prevention					
7	Strengthening fraud investigation processes					
8	Implementing biometric authentication systems					
9	Regular audits and monitoring of high-risk accounts					
10	Strict access control for sensitive systems					