



Electronic Theses and Dissertations

2025

Moderating effect of staff training on determinants of fraudulent practices committed by bank employees in Kenyan commercial banks.

Robi, Joseph Magige
Strathmore Business School
Strathmore University

Recommended Citation

Robi, J. M. (2025). *Moderating effect of staff training on determinants of fraudulent practices committed by bank employees in Kenyan commercial banks* [Strathmore University]. <http://hdl.handle.net/11071/15757>

Follow this and additional works at: <http://hdl.handle.net/11071/15757>

**MODERATING EFFECT OF STAFF TRAINING ON DETERMINANTS OF
FRAUDULENT PRACTICES COMMITTED BY BANK EMPLOYEES IN
KENYAN COMMERCIAL BANKS**

JOSEPH MAGIGE ROBI

169104



**RESEARCH THESIS SUBMITTED TO STRATHMORE UNIVERSITY
BUSINESS SCHOOL IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF A MASTER OF COMMERCE (MCOM) DEGREE,
FORENSIC ACCOUNTING OPTION.**

**STRATHMORE UNIVERSITY BUSINESS SCHOOL
STRATHMORE UNIVERSITY
NAIROBI, KENYA.**

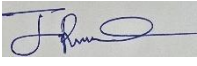
May 2025

DECLARATION

I affirm that this work has not been submitted or approved for the conferment of a degree at this or any other university. To the best of my knowledge, the proposal does not contain any content previously published or written by someone else, except where proper citation has been provided.

Name: Joseph Magige Robi

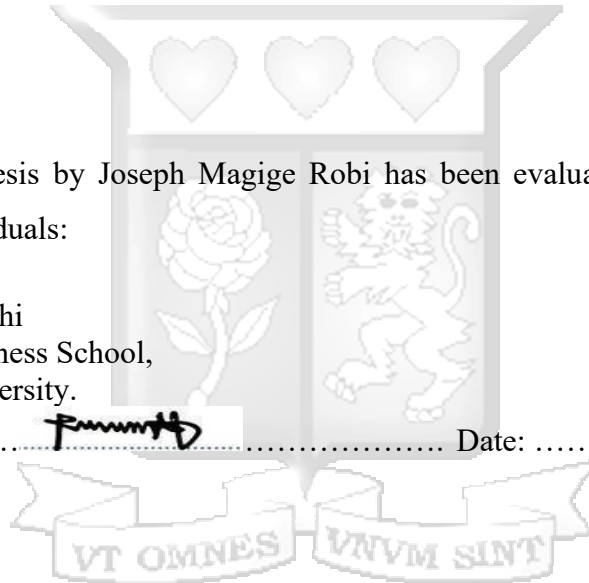
Adm no: 169104

Signature:  Date: ...20/5/2025.....

The research thesis by Joseph Magige Robi has been evaluated and approved by the following individuals:

Dr. Erastus Mbithi
Strathmore Business School,
Strathmore University.

Signature:  Date:19/5/25.....



ABSTRACT

In the modern financial landscape, fraudulent practices in commercial banks pose a critical challenge to financial stability, regulatory compliance, and customer trust. This study examines the determinants of fraudulent practices among employees in Kenyan commercial banks, focusing on internal control systems, regulatory compliance, organizational culture, and technological advancements. The aim of this study was to evaluate the effectiveness of various factors in preventing fraudulent activities and maintaining the integrity of banking operations. The research is based on the Fraud Triangle Theory, Fraud Diamond Theory, Social Learning Theory and Routine Activity Theory, which offer valuable insights into the motivations and opportunities for fraud within financial institutions. A positivist approach is taken, employing an explanatory research design. Primary data was gathered through structured questionnaires directed at bank managers involved in risk management, compliance, internal auditing, and governance across Kenya's 38 licensed commercial banks. A total of 152 participants were selected using a census sampling method and the data was analyzed through both descriptive and inferential statistical techniques to uncover patterns and relationships among the variables. The study findings reveal that Kenyan commercial banks have effective internal control systems, comply with regulatory requirements, foster a strong ethical culture and utilize advanced technologies to prevent fraud. The study further reveals that there was a strong positive correlation between internal control, regulatory compliance, organizational culture, technological advancements, staff training and fraud detection. The study concludes that robust internal control systems, regulatory compliance, a strong ethical culture, and the use of advanced technologies are key factors in reducing fraudulent practices in Kenyan commercial banks. It is recommended that Kenyan commercial banks enhance their whistleblowing mechanisms, invest in regular employee training on fraud prevention, and further strengthen their internal control systems. Additionally, banks should continue to adopt innovative technologies and foster a culture of ethics and transparency to minimize fraud risks.

VT OMNES VNVM SINT

TABLE OF CONTENTS

DECLARATION	ii
ABSTRACT	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	ix
TABLE OF FIGURES	x
LIST OF ABBREVIATIONS	xi
ACKNOWLEDGMENT	xii
DEDICATION	xiii
CHAPTER ONE	1
INTRODUCTION	1
1.1 Background of the Study.....	1
1.1.1 Fraudulent Practices in Commercial Banks	2
1.1.2 Determinants of Fraudulent Practices in Commercial Banks	2
1.1.3 Staff Training	3
1.1.4 Commercial Banks in Kenya	5
1.2 Statement of the Problem.....	8
1.3 Research Objective.....	10
1.3.1 General Objective.....	10
1.3.2 Specific Objectives.....	10
1.4 Research Questions	10
1.5 Scope of the Study	11
1.6 Significance of the Study	11
1.6.1 Bank Managers.....	11
1.6.2 Regulatory Bodies.....	12

1.6.3 Policymakers	12
1.6.4 Academics and Scholars	12
1.6.5 Financial Institutions	12
1.7 Chapter Summary.....	13
CHAPTER TWO	14
LITERATURE REVIEW.....	14
2.1 Introduction.....	14
2.2 Theoretical Framework.....	14
2.2.1 Fraud Triangle Theory	15
2.2.2 Fraud Diamond Theory.....	17
2.2.3 Social Learning Theory.....	18
2.2.4 Routine Activity Theory	20
2.3 Empirical Literature Review.....	23
2.3.1 Internal Control Systems and Fraudulent Practices	23
2.3.2 Regulatory Compliance and Fraudulent Practices	26
2.3.3 Organizational Culture and Fraudulent Practices	28
2.3.4 Technological Advancements and Fraudulent Practices.....	31
2.3.5 Moderating Effect of Staff Training on Fraudulent Practices.....	34
2.4 Research Gap	36
2.5 Conceptual Framework.....	43
2.6 Operationalization of study variables	47
2.7 Chapter Summary.....	49
CHAPTER THREE	50
RESEARCH METHODOLOGY	50
3.1 Introduction.....	50

3.2 Research Philosophy	50
3.3 Research Design.....	51
3.4 Population	52
3.5 Sampling	53
3.5.1 Sampling Frame	53
3.5.2 Sampling Technique.....	53
3.6 Data Collection Methods	54
3.7 Data Collection Procedure	55
3.8 Data Analysis	55
3.8.1 Diagnostic Tests.....	59
3.9 Research Quality	59
3.9.1 Validity of Research Instruments.....	59
3.9.2 Reliability of Research Instruments.....	60
3.10 Ethical Considerations	60
3.11 Chapter Summary.....	61
CHAPTER FOUR.....	62
PRESENTATION OF FINDINGS.....	62
4.0 Presentation of Findings.....	62
4.1 Response Rate	62
4.2 Pilot Study Results	62
4.2.1 Reliability Test.....	62
4.3 Demographic information	63
4.3.1 Gender of the Respondents	63
4.3.2 Age Bracket of the Respondents	64
4.3.3 Education Level of the Respondents.....	64

4.3.4 Job position of the Respondents.....	65
4.3.5 Employment Type of the Respondents	66
4.3.6 Years of Working in the Banking Sector	66
4.3.7 Bank Tier Number of the Respondents.....	67
4.4 Descriptive Analysis	67
4.4.1 Descriptive statistics Findings for Internal Control Systems.....	68
4.4.2 Descriptive Statistics Findings for Regulatory Compliance	72
4.4.3 Descriptive Statistics Findings for Organizational Culture	75
4.4.4 Descriptive Statistics Findings for Technological Advancement	79
4.4.5 Descriptive Statistics Findings for Fraudulent Practices	84
4.4.6 Descriptive statistics Findings for staff training	89
4.5 Inferential Statistics.....	93
4.5.1 Linearity Test	93
4.5.2 Homoscedasticity Test.....	94
4.4.3 Normality Test	95
4.4.4 Multicollinearity Test.....	96
4.5 Correlation Analysis.....	96
4.6 Hierarchical Moderated Regression Analysis.....	98
4.7 Chapter summary	103
CHAPTER FIVE.....	105
SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS ..	105
5.1 Introduction.....	105
5.2 Summary of the Study Findings.....	105
5.2.1 Effect of internal control systems	105
5.2.2 Effect of regulatory compliance.....	105

5.2.3 Effect of organizational culture.....	106
5.2.4 Effect of technological advancements	106
5.2.5 Staff training.....	107
5.3 Discussion	107
5.3.1 Effect of internal control systems	107
5.3.2 Effect of regulatory compliance.....	108
5.3.3 Effect of organizational culture.....	110
5.3.4 Effect of technological advancements	112
5.3.5 Staff training.....	114
5.4 Conclusion	116
5.5 Recommendations of the study	118
5.6 Limitation of the study.....	119
5.7 Suggestion for the study.....	119
5.8 Chapter summary	120
REFERENCES.....	122
APPENDICES	142
APPENDIX I INTRODUCTION LETTER	142
APPENDIX II QUESTIONNAIRE	143
APPENDIX III: LIST OF COMMERCIAL BANKS	149
APPENDIX IV: ETHICAL REVIEW APPROVAL LETTER.....	151
APPENDIX VI: RESEARCH LICENSE	152

LIST OF TABLES

Table 2.1 Summary of Literature and Research Gaps	39
Table 2.2: Operationalization of Variables	47
Table 3.1 Target population	52
Table 3.2 Sample size distribution	53
Table 4.1 Response Rate	62
Table 4.2 Reliability Test	62
Table 4.3 Gender of the Respondents	64
Table 4.4 Age Brackets of the Respondents	64
Table 4.5 Education Level of the Respondent	65
Table 4.6 Job Position of the Respondents	65
Table 4.7 Employment Type of the Respondents	66
Table 4.8 Years of Working in the Banking Sector	66
Table 4.9 Bank Tier Number of the Respondents	67
Table 4.10 Descriptive statistics Findings for Internal Control Systems	68
Table 4.11 Descriptive Statistics Findings for Regulatory Compliance	72
Table 4.12 Descriptive Statistics Findings for Organizational Culture	75
Table 4.13 Descriptive Statistics Findings for Technological Advancement	79
Table 4.14 Descriptive Statistics Findings for Fraudulent Practices	84
Table 4.15 Descriptive statistics Findings for staff training	89
Table 4.16 Test of Linearity	93
Table 4.17 Homoscedasticity Assumption	94
Table 4.18 Normality Assumption Test	95
Table 4.19 Multicollinearity Test	96
Table 4.20 Correlation Analysis	97
Table 4.21 Hierarchical Moderated Regression Analysis	99

TABLE OF FIGURES

Figure 2.1 Conceptual Framework.....45



LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AML	Anti-Money Laundering
BFID	Banking Fraud Investigations Department
CBK	Central Bank of Kenya
CMA	Capital Markets Authority
COSO	Committee of Sponsoring Organizations of the Treadway Commission
GDP	Gross Domestic Product
IMF	International Monetary Fund
KDIC	Kenya Deposit Insurance Corporation



ACKNOWLEDGMENT

I want to show deep appreciation to God Almighty because He gave me the power along with endurance and intelligence needed to finish this research study.

Dr. Erastus Mbithi receives my most heartfelt appreciation because he provided exceptional supervision throughout my research project with his valuable advice and ongoing backing. His professional expertise led to substantial improvements in the quality of this work.

Strathmore University Business School receives my sincere appreciation for offering an outstanding academic setting together with essential resources that helped me finalize this research work.

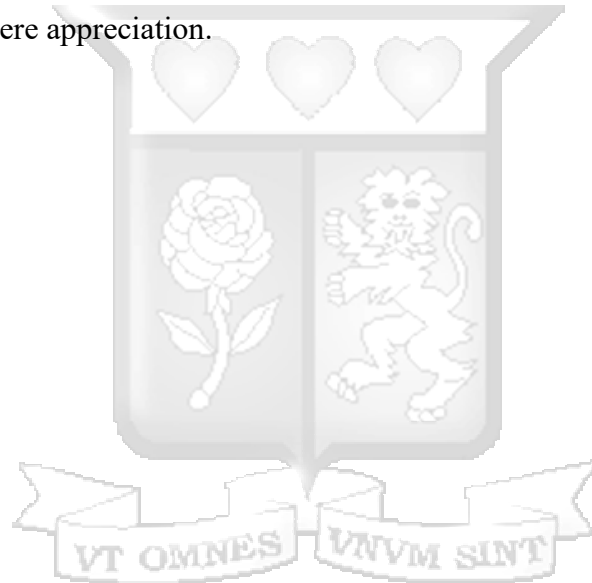


DEDICATION

The research study I conduct goes to my dear family because they provide unwavering support and encouragement that serves as my biggest driving force.

The depth of my gratitude extends to my parents because they sacrificed themselves while loving me without limits and continuously believing in what I could achieve. Your direction proved essential in my academic development as well as my professional progress.

Your endless support together with your patience and uplifting words defines everything to my family and my friends. Your love combined with trust for my academic journey receives my sincere appreciation.



CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The 21st-century global financial landscape is characterized by rapid transformation, driven by globalization, technological advances, and evolving regulatory standards (Yoganandham, 2024). This transformation has led to an increasing complexity in financial systems, heightening the risk of fraudulent practices that undermine institutional stability and public trust. Fraudulent activities, which include deliberate misrepresentations and actions carried out with dishonest intentions, are a critical concern for financial systems worldwide (Sukmadilaga et al., 2022). These activities are perpetrated with the aim of obtaining unauthorized financial benefits or avoiding obligations, posing significant risks to the economy (Adekunle & Olusa, 2021). The Association of Certified Fraud Examiners (ACFE) describes fraud as actions that involve deceit, manipulation, or trickery to achieve financial gain, highlighting its significance as a major threat to economic stability. To address these issues, global institutions like the International Monetary Fund (IMF) advocate for robust regulatory frameworks and fraud detection systems to ensure financial stability (IMF, 2021).

Countries globally have developed different strategies to combat fraud. For instance, the United States has reduced fraud rates through advancements in analytics and biometric security (Federal Reserve, 2023). Similarly, the UK's Financial Conduct Authority (2022) has enforced stringent digital verification measures, which have led to a significant decline in online banking fraud. In Asia, nations like China and India have increased cybersecurity efforts to combat rising cyber fraud (Huang et al., 2022). In Africa, responses to fraud vary, with countries like Nigeria grappling with weak regulatory enforcement (Onyeama, 2024), while South Africa has made notable strides in integrating security technologies and regulatory frameworks (South African Reserve Bank, 2022).

Kenya's banking sector faces similar challenges with a rise in fraudulent activities, including cybercrimes and internal collusion (BFID, 2022). The Central Bank of Kenya (CBK, 2023) has implemented new guidelines to strengthen oversight, particularly in the digital banking sector, but the persistent threat of fraud highlights the need for continuous

improvement in detection and prevention strategies to protect public trust and maintain financial stability (Anyona, 2024).

1.1.1 Fraudulent Practices in Commercial Banks

Fraudulent practices in commercial banks have evolved significantly, with employees, customers, and management being implicated (Ametepe et al., 2023). Employee fraud, also known as occupational fraud, is one of the most prevalent forms, with employees abusing their positions for financial gain. In addition to this, customer fraud, which includes activities like account takeovers and credit card fraud, remains a major threat in commercial banking. Management fraud, though less frequent, also occurs, particularly in cases where senior officials manipulate financial reports or engage in illicit financial dealings to benefit from corporate resources (Grandstaff & Solsma, 2021). Understanding the nature and scope of these fraudulent activities is critical to designing effective prevention strategies.

Statistics indicate a rising trend in fraud cases across Kenya's banking sector. The Banking Fraud Investigations Department (BFID, 2022) reported a notable increase in the frequency of fraud-related cases in recent years, particularly in cybercrime. The number of fraud cases in Kenyan banks rose by approximately 30% from 2021 to 2022, with the value of fraud-related losses estimated at over KES 3 billion (Kenya Bankers Association, 2022). This increase is attributed to the rapid adoption of digital banking services, which, while offering convenience, have also exposed banks to cyber threats. In addition, internal fraud, including cases of collusion between employees and customers, has also contributed to this rise. The recent surge in mobile banking fraud, such as SIM card swapping and phishing attacks, highlights the vulnerabilities in Kenya's increasingly digital financial services sector. In this study, fraudulent practices refer to intentional deceptive actions by bank employees aimed at personal gain, with key determinants including inadequate staff training, weak internal controls, poor organizational culture, pressure to meet targets, compliance gaps, and governance deficiencies.

1.1.2 Determinants of Fraudulent Practices in Commercial Banks

Several key determinants contribute to the prevalence of fraudulent practices in commercial banks. These include internal control systems, regulatory compliance,

organizational culture, and technological advancements. All four of these determinants are preventative in nature (Mulugeta, 2021). They aim to proactively address potential fraud by implementing systems, compliance measures, cultural frameworks, and technological solutions that reduce the likelihood of fraud occurring. While they are designed to prevent fraud, if they fail, they may also have corrective functions, such as identifying and addressing fraud after it has occurred, but their primary purpose is to act as preventative measures (Rashid et al., 2022).

Internal controls, designed to monitor and manage operations, are considered one of the most effective methods for fraud prevention (COSO, 2013). However, their effectiveness is contingent upon factors like management commitment and organizational culture (Vutumu et al., 2021). Additionally, regulatory compliance defined as adherence to laws, regulations, and ethical guidelines governing banking operations has been identified as a crucial component in curbing fraudulent practices (Blair & Barbiani, 2019). While regulatory frameworks are essential, their effectiveness is compromised by weak enforcement and inconsistent implementation (Olojede et al., 2020).

Organizational culture also plays a significant role in mitigating fraud. A culture of transparency, accountability, and ethical practices within an institution reduces the likelihood of fraud (Hasham et al., 2019). However, the effectiveness of organizational culture in reducing fraud is debated, with some studies suggesting that culture alone may not be enough unless combined with strong governance structures (Onyancha, 2023). Technological advancements, such as AI and predictive analytics, have also become integral in addressing modern fraud risks, particularly in highly digitized banking environments (Rai & Acharya, 2021; Hasham et al., 2019). However, the evolving nature of fraud also poses challenges, as fraudsters continuously adapt their tactics to circumvent detection (Bhatt et al., 2023).

1.1.3 Staff Training

Staff training is emerging as a vital factor in enhancing the effectiveness of fraud prevention strategies (Kaur et al., 2023). While internal controls, regulatory compliance, and organizational culture are essential, they can be undermined by a lack of awareness and skills among employees. Comprehensive staff training programs equip employees

with the necessary tools to recognize and respond to fraud effectively (Bishop, 2022). These programs focus on fostering an understanding of ethical standards, compliance protocols, and the latest fraud prevention technologies, ensuring that employees play a proactive role in safeguarding the financial institution. However, the effectiveness of these programs in reducing fraud in Kenyan banks remains underexplored, particularly in how they can strengthen existing deterrents like internal controls and compliance measures (Oguya, 2024).

Staff training has long been recognized as an essential factor in enhancing the effectiveness of fraud prevention strategies. While traditional measures such as internal controls, regulatory compliance, organizational culture, and technological advancements are vital in combating fraud, the effectiveness of these measures can be significantly augmented when employees are equipped with the necessary skills and awareness (Kuruppu et al., 2021). Staff training ensures that employees understand not only the importance of these systems but also how to engage with them effectively. Therefore, staff training should be treated as a moderating variable because it interacts with these existing fraud prevention factors, enhancing their ability to prevent fraud in the workplace (Njuguna et al., 2021).

The theoretical foundations of Fraud Triangle Theory, Fraud Diamond Theory, Social Learning Theory, and Routine Activity Theory provide strong support for considering staff training as a moderator. Fraud Triangle Theory asserts that fraud occurs when three elements—pressure, opportunity, and rationalization—are present (Owusu et al., 2022). In this framework, staff training can moderate the opportunity for fraud by enhancing employees' understanding of internal controls and ethical conduct, thereby reducing the chances of fraud. Similarly, Social Learning Theory explains that employees learn behaviors from observing peers and organizational leaders. Well-designed training programs can instill ethical behavior and discourage fraudulent conduct, reinforcing a positive organizational culture (Smith & Kouchaki, 2021). Lastly, Routine Activity Theory posits that fraud occurs when motivated offenders find suitable targets in the absence of capable guardians. Staff training enhances employees' role as guardians by ensuring they can effectively monitor activities and prevent fraud (Mabunda, 2024).

Empirically, existing studies have shown that staff training not only improves employees' skills and awareness but also enhances the effectiveness of fraud detection and prevention measures. Research by Kaur et al. (2023) and Bishop (2022) suggests that training programs significantly improve employees' ability to recognize fraud, adhere to compliance measures, and use fraud detection technologies. However, while training is often viewed as an independent factor, its moderating role has been less explored. The current study aims to address this gap by demonstrating how staff training moderates the relationship between fraud prevention measures and fraud occurrence. The results suggest that staff training interacts with internal controls, regulatory compliance, organizational culture, and technological advancements to increase their effectiveness in reducing fraud.

This study contributes new insights to the literature by showing that staff training does not merely complement fraud prevention measures but actively enhances their impact. The findings indicate that when staff are well-trained, they are better equipped to engage with existing fraud prevention strategies and adapt to emerging threats. In the context of Kenyan commercial banks, this research highlights the critical importance of integrating staff training into fraud prevention frameworks. It suggests that banks should invest in continuous, comprehensive training programs that not only focus on compliance but also foster a culture of ethical behavior and proactive fraud detection (Kimani & Kibera, 2023). Staff training should be treated as a moderating variable because it significantly influences the effectiveness of other fraud prevention strategies. This study strengthens the theoretical and empirical justification for viewing training as a moderating factor and offers practical recommendations for improving fraud prevention in the banking sector. By recognizing the moderating role of staff training, banks can more effectively mitigate fraud risks and enhance the overall security of their operations.

1.1.4 Commercial Banks in Kenya

The evolution of commercial banks in Kenya has been marked by substantial growth and change, particularly following the liberalization of the financial sector in the 1990s. This period marked the emergence of indigenous banks aimed at serving the financial needs of local businesses and populations, shifting from a sector previously dominated by foreign-owned institutions (Kamau & Were, 2018). Technological advancements, notably the

introduction of mobile banking and fintech solutions in the early 2000s like Mpesa, have revolutionized the banking landscape, promoting financial inclusion and accessibility (Muthinja & Chipeta, 2018). In recent years, Kenyan banks have expanded regionally, contributing to East African economic integration and showcasing the sector's dynamism and adaptability (Wachira & Ondigo, 2018).

The regulation of commercial banks in Kenya is chiefly overseen by the Central Bank of Kenya (CBK), which was established under the Central Bank of Kenya Act (Owino, 2019). The CBK formulates monetary policy, promotes financial stability, and supervises banks to ensure compliance with statutory requirements and international best practices (Mwega, 2016). In response to challenges such as financial crises and technological changes, the CBK has implemented stringent regulatory frameworks, including risk-based supervision and enhanced corporate governance guidelines (Waweru & Kalani, 2019). The Central Bank of Kenya (CBK) also works in conjunction with other regulatory bodies, such as the Capital Markets Authority (CMA) and the Kenya Deposit Insurance Corporation (KDIC), to ensure the integrity of the financial system (Kariuki & Muturi, 2015).

As of 2023, Kenya's commercial banking sector comprises 38 licensed banks, categorized into tiers based on asset size and market share (Central Bank of Kenya, 2023). Tier I banks such as KCB Group, Equity Bank, and Cooperative Bank control a significant portion of the market, holding over 50% of the industry's total assets (Mwangi & Muturi, 2016). Tier II banks are medium-sized institutions with a moderate market presence, while Tier III banks are smaller and often serve niche markets or specific regions (Kiplangat et al., 2019). The banking sector is a vital contributor to Kenya's Gross Domestic Product (GDP), accounting for approximately 6% through financial intermediation, capital formation, and facilitation of trade and investment (Ngugi & Nyang'oro, 2017). By mobilizing savings and extending credit, commercial banks stimulate economic activities across various sectors, driving economic growth and development (Wambua & Mugambi, 2019).

Kenya's banking sector has experienced notable growth in recent years, particularly with the expansion of digital banking. However, this growth has also led to an increased

vulnerability to fraud. The Central Bank of Kenya (CBK) (2023) has introduced various guidelines to improve security in digital transactions, yet challenges persist, including insufficient staff training and evolving fraudulent tactics. Additionally, the sector has struggled to fully align with international best practices, such as advanced fraud detection technologies and regulatory compliance standards (Chitai et al., 2024). The lack of in-depth research on fraud determinants within the Kenyan banking context presents a gap that this study seeks to address.

Numerous empirical studies have highlighted key determinants contributing to the prevalence of fraudulent activities in commercial banks, including internal control systems, regulatory compliance, organizational culture, and technological advancements. These factors primarily function as preventative measures designed to proactively address potential fraud (Mulugeta, 2021). Internal controls play a critical role in monitoring and managing banking operations, while regulatory compliance ensures adherence to laws and ethical standards (Blair & Barbiani, 2019). Additionally, organizational culture that promotes transparency and ethical behavior, alongside technological innovations such as AI and predictive analytics, are vital in curbing fraud (Rai & Acharya, 2021).

However, despite the implementation of these strategies, fraud continues to be a persistent challenge in Kenya's banking sector. Recent reports indicate a rising trend in reported fraud cases, with the Central Bank of Kenya noting a significant increase in financial losses due to employee-related fraud over the past five years (CBK Annual Report, 2024). This persistence suggests that existing measures alone are insufficient in effectively preventing fraud. Empirical evidence points to a gap in addressing critical factors such as employee awareness, skills, and behavior in fraud prevention efforts.

Staff training has emerged as a key factor in strengthening fraud prevention strategies (Kaur et al., 2023). While internal controls, regulatory compliance, organizational culture, and technology remain essential, their effectiveness heavily relies on how well employees understand and implement them. Training equips employees with the necessary knowledge and skills to recognize and respond to fraud risks effectively. Nonetheless, the moderating role of staff training—how it enhances the effectiveness of these fraud

prevention measures—remains underexplored, particularly within the context of Kenyan commercial banks.

This study aims to fill this empirical gap by investigating staff training as a moderator that can amplify the impact of internal control systems, regulatory compliance, organizational culture, and technological advancements on fraud reduction. Staff training not only improves employees' ability to implement controls and comply with regulations but also fosters a culture of transparency and optimizes the use of advanced fraud detection technologies. Consequently, staff training should not be viewed as a standalone solution but as an integral component that strengthens existing fraud prevention frameworks.

Despite a substantial body of literature on fraud prevention, few empirical studies have examined the moderating effect of staff training in enhancing the effectiveness of fraud deterrents. By exploring this interaction, the current study contributes new insights into more effective implementation of fraud prevention strategies aimed at combating the persistent fraud challenges in Kenya's banking sector.

1.2 Statement of the Problem

Kenyan commercial banks continue to face increasingly sophisticated fraudulent practices, despite significant investments in advanced regulatory frameworks and technological solutions. The 2023 report by the Central Bank of Kenya (CBK) underscores the severity of this issue, revealing substantial financial losses within the banking sector due to fraud tactics such as identity theft, electronic funds transfer fraud, and document forgery. In the first half of 2023 alone, Kenyan banks reported losses amounting to approximately \$9.4 million due to these fraudulent schemes (CBK, 2023). A notable case is a financial breach at Absa Bank Kenya, which incurred a loss of Sh107.7 million in 2023, despite the bank's comprehensive fraud prevention measures, including staff training and customer awareness programs. These incidents expose the limitations of current fraud prevention strategies, raising questions about their sufficiency in fully countering the evolving nature of fraudulent activities.

This problem is not confined to Kenya alone. On a global scale, even advanced economies continue to grapple with the challenge of containing fraud, despite substantial investments

in technological and regulatory measures. For example, reports from the United States and the European Union indicate a rise in cyber-enabled financial crimes, where criminals employ increasingly advanced techniques to bypass traditional regulatory controls. The European Central Bank (2022) has highlighted the difficulties of managing cross-border fraud, further emphasizing the inadequacies of existing fraud prevention frameworks. The persistence of these challenges worldwide suggests that a multi-faceted approach, integrating regulatory compliance, organizational culture, and technological solutions, is essential to effectively combat modern fraud (AL-Hawamleh, 2024).

In Sub-Saharan Africa, including Kenya, studies reveal specific weaknesses in fraud prevention strategies, particularly in areas such as internal control systems, regulatory compliance, organizational culture, and technological advancements. For instance, research by Chege and Mutua (2019) emphasizes that internal fraud, especially occupational fraud committed by employees, is closely linked to organizational culture. Furthermore, while the adoption of artificial intelligence (AI) in fraud detection has shown promise (Kiplagat, 2021), these technologies are not yet fully optimized to address all emerging fraud techniques. This indicates a need for continuous refinement and integration of technology in fraud prevention efforts.

Despite the extensive body of literature on fraud prevention, the effectiveness of individual strategies, such as internal controls, regulatory compliance, organizational culture, and technological advancements, remains controversial when applied in isolation. Studies by Fernandhytia and Muslichah (2020) and Olojede et al. (2020) highlight the importance of combining these factors for effective fraud prevention. However, no single approach has proven entirely sufficient, suggesting the necessity of a comprehensive and integrated approach. Additionally, while existing research has largely focused on these individual determinants, there has been limited exploration into the moderating role of staff training in enhancing the effectiveness of these strategies, particularly in the context of Kenyan commercial banks.

This research seeks to address these gaps by exploring the combined influence of internal control systems, regulatory compliance, organizational culture, and technological advancements on fraudulent practices in Kenyan commercial banks. In particular, the

study aims to examine the moderating role of staff training in improving the effectiveness of these existing fraud prevention strategies. By employing a multi-theoretical approach and a mixed-methods design, this study aims to provide a more integrated and practical framework for enhancing fraud prevention measures within Kenya's banking sector.

1.3 Research Objective

1.3.1 General Objective

The primary objective of this study was to evaluate the moderating effect of staff training on the relationship between the factors influencing fraudulent practices among employees in Kenyan commercial banks.

1.3.2 Specific Objectives

- i. To assess the effect of internal control systems on the occurrence of fraudulent practices among employees in Kenyan commercial banks.
- ii. To examine the effect of regulatory compliance on the occurrence of fraud in Kenyan commercial banks.
- iii. To determine the effect of organizational culture on the occurrence of fraudulent activities in Kenyan commercial banks.
- iv. To evaluate the effect of technological advancements on the occurrence of fraud in Kenyan commercial banks.
- v. To establish the moderating effect of staff training on the relationship between determinants of fraudulent practices among employees in Kenyan commercial banks.

1.4 Research Questions

- i. What is the effect of internal control systems on the occurrence of fraudulent practices among employees in Kenyan commercial banks?
- ii. What is the effect of regulatory compliance on the occurrence of fraud in Kenyan commercial banks?
- iii. How does organizational culture affect the occurrence of fraudulent activities in Kenyan commercial banks?
- iv. What is the effect of technological advancements on the occurrence of fraud in Kenyan commercial banks?

- v. Does staff training have a moderating effect on determinants of fraudulent practices among employees in Kenyan commercial banks?

1.5 Scope of the Study

This research focused on Kenyan commercial banks, specifically examining the determinants of fraudulent practices within these institutions. For this study, the sample size includes all 38 commercial banks and one manager from each of the four relevant departments, resulting in a total of 152 respondents. The study was conducted from January 2025 to April 2025. The independent variable was internal control systems, regulatory compliance, organizational culture, and technological advancements and dependent variable occurrence of fraud. Staff training was the moderate variable. Data was collected through primary sources, including structured questionnaires with commercial bank employees. The research aims were to provide insights into the effectiveness of current anti-fraud measures and propose strategies for enhancing fraud prevention and detection within Kenyan commercial banks.

1.6 Significance of the Study

This study will make a significant contribution to the understanding of fraudulent practices in the banking sector, particularly within the context of Kenyan commercial banks. It offers valuable insights to bank managers, regulatory authorities, policymakers and academics on effective strategies to mitigate and prevent fraud. The findings assisted in developing targeted approaches to strengthen the security and integrity of banking operations, ultimately supporting the financial stability and economic growth of the country.

1.6.1 Bank Managers

The study will offer bank managers valuable insights into the effectiveness of their existing internal control systems, regulatory compliance protocols, organizational culture, and technological advancements in combating fraud. By identifying the key factors that contribute to fraudulent activities, bank managers were better equipped to implement stronger fraud prevention and detection strategies. This will help protect the bank's assets, enhance customer trust, and improve overall operational efficiency.

1.6.2 Regulatory Bodies

Regulatory bodies can use the findings of this study to refine and enforce more effective regulatory frameworks that address the specific vulnerabilities of Kenyan commercial banks. Insights into the current compliance levels and the impact of regulatory measures on fraud prevention will enable regulators to develop and implement policies that strengthen the overall security of the banking sector. This can lead to more stringent monitoring and enforcement practices, ensuring that banks adhere to high standards of fraud prevention.

1.6.3 Policymakers

Policymakers can utilize the insights from this study to create and implement comprehensive policies that promote a secure and fraud-resistant banking environment. By understanding the impact of regulatory compliance, organizational culture, and technological advancements on fraud occurrence, policymakers can develop initiatives that support robust internal controls and innovative technological solutions. These policies can contribute to reducing financial crimes, protecting consumers, and fostering economic stability.

1.6.4 Academics and Scholars

The study will contribute to the academic literature on fraud prevention within the banking sector, laying the foundation for further research. Scholars can expand on this work to investigate additional factors influencing fraud and the effectiveness of different prevention strategies. The findings will also be beneficial for educators in developing curricula that address the complexities of financial fraud and emphasize the importance of strong internal controls, compliance, and technological innovation in the banking industry.

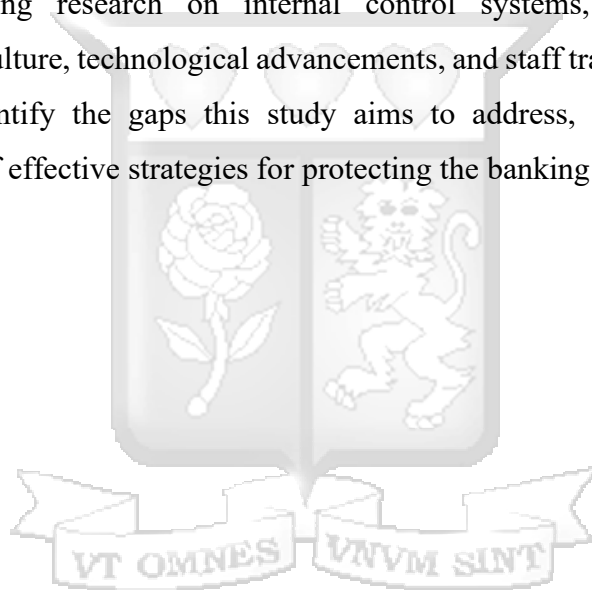
1.6.5 Financial Institutions

Financial institutions will benefit from the detailed analysis of fraud determinants provided by this study. By identifying the key factors that contribute to fraudulent activities, banks can tailor their fraud prevention programs more effectively. This can lead to better risk management practices, reduced financial losses, and enhanced customer confidence. Additionally, the study's insights can help financial institutions develop more

targeted training programs for employees, focusing on fostering a culture of integrity and vigilance against fraud.

1.7 Chapter Summary

This opening chapter offers an overview of the importance of understanding the factors driving fraudulent practices among employees in Kenyan commercial banks. It presents the research problem, objectives, and the study's significance. The chapter discusses the substantial financial losses banks face due to fraud, the challenges created by evolving fraudulent tactics, and the need for comprehensive approaches to strengthen fraud prevention and detection. The next chapter provides an in-depth literature review, exploring existing research on internal control systems, regulatory compliance, organizational culture, technological advancements, and staff training in fraud prevention. It will also identify the gaps this study aims to address, contributing to a deeper understanding of effective strategies for protecting the banking sector from fraud.



CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews existing literature on fraudulent practices in the banking sector and their determinants, with a specific focus on internal control systems, regulatory compliance, organizational culture, and technological advancements also moderating effect of staff training on fraudulent practices. The discussion explores how these factors contribute to the prevalence of fraud within commercial banks in Kenya. Moreover, the chapter identifies key research gaps, outlines a conceptual framework, and provides a chapter summary.

2.2 Theoretical Framework

In the current study on the determinants of fraudulent practices among employees in Kenyan commercial banks, Fraud Triangle Theory, Fraud Diamond Theory, Social Learning Theory, and Routine Activity Theory was essential for analysis. These theories help explore how internal controls, regulatory compliance, organizational culture, and technological advancements influence the occurrence of fraud within these institutions. Among the three theories discussed, Fraud Triangle Theory bears the greatest relevance to the theme of this study and serves as the anchor theory. The primary focus of the study is to investigate the various determinants of fraudulent behavior in Kenyan commercial banks, and Fraud Triangle Theory provides the most comprehensive framework for understanding how opportunity, pressure, and rationalization interact to foster fraud.

This theory not only explains the fundamental causes of fraud but also integrates well with other factors such as internal controls, organizational culture, and staff training. The Fraud Triangle Theory serves as the basis for understanding how these factors interact, particularly in the context of how staff training can moderate the relationships between these factors and the occurrence of fraud. It guides the exploration of how weak internal controls, an unethical culture, and personal pressures converge to create an environment ripe for fraud.

By focusing on these core elements, Fraud Triangle Theory provides the most robust framework for understanding the dynamics of fraud within Kenyan commercial banks,

and it aligns closely with the study's objectives of identifying the determinants of fraud and exploring the moderating role of staff training.

2.2.1 Fraud Triangle Theory

The study was guided by Cressey's Fraud Triangle Theory, developed in 1953 which explains that fraudulent acts stem from the intersection of three key factors: financial or personal strain, perceived opportunity, and the ability to justify the crime (Lau, 2024). This model posits that individuals facing significant pressures, who see a chance to exploit weaknesses in a system, and who can rationalize their unethical behavior, are more prone to commit fraud. Donald Cressey's Fraud Triangle Theory (1953) remains foundational, framing fraudulent practices as an interplay of pressure for example, financial strain, opportunity (weak internal controls), and rationalization (unethical organizational culture) (Lederman, 2019). This aligns with Kenya's banking sector, where lax oversight (internal controls) and profit-driven cultures (organizational culture) create fertile ground for fraud. Wolfe and Hermanson's Fraud Diamond Theory adds capability such as technical skills to exploit systems, linking directly to technological advancements, a double-edged sword where innovations like AI can deter fraud but also introduce vulnerabilities if poorly managed (Soneji, 2022).

The Fraud Scale Theory (Awodiran, 2022) introduces situational pressures such as unrealistic targets and personal integrity, tying to Kenya's high-pressure banking environments where aggressive sales cultures and employee financial instability escalate fraud risks. The COSO Framework (2013) emphasizes internal control systems as critical to fraud prevention, directly linking to Kenya's need for robust oversight mechanisms (Opiyo, 2023). Weaknesses in controls such as poor segregation of duties amplify opportunities, as seen in the 2016 Imperial Bank scandal. M.I.C.E. Theory (Money, Ideology, Coercion, Ego) expands on Cressey's "pressure" by incorporating non-financial motives such as ideological sabotage, relevant to Kenya's politically connected banks where coercion or ego-driven fraud may occur.

Technological advancements further complicate the landscape: while blockchain can enhance transparency; reducing opportunity, rapid digitization in Kenya's banking sector such as mobile money platforms like M-Pesa have outpaced cybersecurity frameworks,

creating new fraud vectors. Deterrence Theory (Ssekubwa, 2022) underscores the role of regulatory compliance in shaping cost-benefit calculations; weak penalties in Kenya's Banking Act, for instance, reduce the perceived cost of fraud.

The Fraud Triangle Theory delivers relevant guidance to explain situations that generate fraudulent activities in Kenyan commercial banks. An investigation of institutional pressures together with analysis of existing opportunities and rationalization methods will help identify the main vulnerabilities which subsequently allow for strategic recommendations regarding fraud risk mitigation. Better internal controls together with identified employee pressure strategies will develop a safer banking environment. Such knowledge enables stakeholders to create solutions for particular weak spots through specific preventative measures which will establish an integrated approach to bank fraud protection.

Fraud Triangle Theory (Cressey, 1953) is foundational to this study as it explains the conditions under which fraudulent behavior occurs, emphasizing the interaction between three factors: pressure, opportunity, and rationalization. The theory suggests that fraud is likely when individuals experience personal or financial pressure, perceive opportunities to exploit weaknesses in the system, and can rationalize their actions, thus making them more willing to engage in fraudulent activities.

In the context of Kenyan commercial banks, Fraud Triangle Theory is particularly relevant to understanding how internal control systems and organizational culture contribute to fraudulent behavior. Weak internal controls create opportunities for employees to commit fraud, while organizational culture may normalize unethical behavior, allowing employees to rationalize their actions. For instance, a profit-driven culture or aggressive sales targets may create pressure, while weak oversight mechanisms allow for rationalization and exploitation of the system.

The theory is connected to Objective i, which aims to assess the effect of internal control systems on the occurrence of fraudulent practices, as weak internal controls provide opportunity for fraud. Objective iii, which explores the effect of organizational culture on fraud, is also aligned with Fraud Triangle Theory, as the theory suggests that a permissive

culture increases the likelihood of rationalization of fraudulent acts. Furthermore, Objective v, which examines the moderating effect of staff training, ties into Fraud Triangle Theory by showing how training can reduce the opportunity for fraud and address the rationalization element by promoting ethical behavior.

2.2.2 Fraud Diamond Theory

The study was guided by the Fraud Diamond Theory developed by David T. Wolfe and Dana R. Hermanson in 2004 as an enhancement to the classic Fraud Triangle theory proposed by Donald Cressey in the 1950s. While the Fraud Triangle identifies three necessary elements for fraud—pressure, opportunity, and rationalization—Wolfe and Hermanson argued that these do not fully explain why some individuals commit fraud and others do not, even when exposed to the same conditions. To address this limitation, they introduced a fourth element, capability, which reflects an individual's personal traits and abilities needed to exploit an opportunity and carry out fraud successfully (Wolfe & Hermanson, 2004).

Pressure refers to external or internal motivations such as financial difficulties that push an individual towards fraudulent behavior. Opportunity involves weaknesses or gaps in organizational controls that allow fraud to occur undetected. Rationalization is the cognitive process where fraudsters justify their behavior as acceptable. Finally, capability includes the knowledge, position, skills, and psychological characteristics that empower individuals to execute fraudulent acts effectively. This addition recognizes that only individuals with the capability to exploit an opportunity will commit fraud (Dorminey et al., 2012).

The Fraud Diamond Theory provides a comprehensive lens to examine fraudulent practices by employees in Kenyan commercial banks, directly relating to the study's objectives. Internal control systems are aimed at reducing the opportunity for fraud by limiting employee access to sensitive information and assets. Effective internal controls create barriers that prevent employees from exploiting system weaknesses, thus mitigating fraud risks (COSO, 2013). Regulatory compliance influences the rationalization component by establishing strict rules, ethical codes, and legal requirements that make it difficult for employees to justify fraudulent behavior. Compliance frameworks foster

accountability and reinforce the consequences of unethical actions, thereby deterring fraud (Blair & Barbiani, 2019).

Organizational culture shapes the ethical climate of the institution, affecting employees' perceptions and moral judgments. A culture that prioritizes transparency, integrity, and accountability reduces the likelihood of rationalizing fraud, encouraging ethical conduct throughout the organization (Kaptein, 2011). Technological advancements impact both opportunity and capability. Advanced technologies such as artificial intelligence and predictive analytics detect irregularities and reduce opportunities for fraudulent acts. Simultaneously, technology enhances employees' capability by providing tools that facilitate the identification and prevention of fraud (Rai & Acharya, 2021).

The study's focus on the moderating effect of staff training highlights the crucial role of enhancing employee capability. Training empowers employees with the knowledge and skills to understand internal controls, comply with regulations, uphold ethical standards, and effectively use technology in fraud detection and prevention. By improving employees' capacity to execute these measures, staff training amplifies the effectiveness of fraud deterrence strategies (Kaur et al., 2023; Wolfe & Hermanson, 2004).

2.2.3 Social Learning Theory

Social Learning Theory was developed by Edwin H. Sutherland in 1939 and later expanded by Ronald Akers in the 1960s. Social Learning Theory posits that criminal or deviant behavior is learned through social interactions with others. Rather than being an inherent trait, criminal behavior is learned through communication, socialization, and the observation of others, particularly those within an individual's immediate environment (Archer & Flexon, 2022). The theory states that deviant behaviors are reinforced when they are rewarded or go unpunished. Positive reinforcement from peers or supervisors can encourage the continuation of such behavior.

In the context of employee fraud in Kenyan commercial banks, Social Learning Theory can be applied to understand how employees learn and adopt fraudulent behaviors. Employees may not engage in fraudulent practices in isolation but are influenced by their social interactions and the culture within the organization (van Steenbergen & Ellemers,

2021). These social interactions could occur with colleagues, supervisors, or even management. The theory can help explain the following aspects, employees who interact with others who normalize or justify fraudulent behavior are more likely to adopt similar attitudes and behaviors. If fraud is perceived as being tolerated or even rewarded, employees may see it as acceptable and might replicate these behaviors to gain benefits, even if they are aware of the associated risks. Employees might adopt fraudulent practices by learning rationalizations for their behavior (Awalluddin et al., 2022). For example, if an employee sees colleagues rationalizing that they "deserve" to steal due to low pay or that "everyone is doing it," they may justify similar actions. If employees witness peers engaging in fraud without facing disciplinary action, they might believe that fraud is risk-free or even permissible, reinforcing their inclination to participate in fraudulent activities themselves. Employees may imitate the behavior of others, especially if those engaging in fraudulent practices appear to succeed or gain rewards for their actions. If management or influential employees display unethical behavior, it might serve as a model for other employees to follow (Soneji, 2022).

By using Social Learning Theory, the study explored how organizational culture, peer behavior, and the social context within the workplace influence employees' decisions to commit fraud. The theory underscores the idea that fraud is not merely a result of individual motivations (as explained in the Fraud Triangle) but is heavily influenced by socialization processes within the organization (Lau, 2024). Thus, combating fraud requires addressing not only individual behavior but also the broader social environment that normalizes or encourages fraudulent actions.

Social Learning Theory (Sutherland, 1939; Akers, 1960) explains that criminal behavior, including fraud, is learned through interactions with others in the environment. It posits that individuals adopt deviant behavior by observing others, particularly peers, supervisors, or role models within their social circle. Positive reinforcement, or the lack of punishment for unethical behavior, encourages the continuation of such practices.

In Kenyan commercial banks, Social Learning Theory is highly applicable to Objective iii and Objective v. Organizational culture plays a crucial role in shaping employees' behaviors, as fraud is often learned by observing peers or management who either engage

in or tolerate fraudulent behavior. If employees observe colleagues engaging in fraud without facing consequences, they may perceive such behavior as acceptable and adopt similar actions.

Staff training plays a moderating role in this process, as Objective v seeks to establish the moderating effect of training. Training programs can alter employees' learned behaviors by reinforcing ethical standards and demonstrating the consequences of unethical actions. By shaping the social environment within the organization, staff training can ensure that employees are socialized into ethical practices, thereby reducing the likelihood of fraud being learned and replicated.

2.2.4 Routine Activity Theory

The Routine Activity Theory proposed by Cohen and Felson (1979) explains that criminal acts develop when motivated offenders meet targets while guardians fail to protect (Reyns, 2025). This theory focuses on the situational context of crime rather than inherent offender traits. Building upon this foundation, scholars like Henson (2020) have broadened the theory to incorporate the influence of daily routines in generating criminal opportunities. These routines, they argue, are key to developing effective crime prevention strategies. For example, Jones and Pridemore (2019) have utilized this theory in the context of urban crime prevention, while Krishnakumar and Verma (2021) have applied it to the study of cybercrime.

In the Kenyan banking landscape, Ngotho (2023) explored how regular banking operations inadvertently create opportunities for fraudulent activities, demonstrating the practical implications of RAT within this environment (Kaunda 2021). The study revealed that routine activities, such as cash handling, loan processing, and customer transactions, often lack sufficient oversight, making banks attractive targets for fraud. This observation aligns with Ammirato et al. (2021), who noted that the routines within retail environments, characterized by inadequate security measures, present actionable insights applicable to banks. The commonality of certain banking activities reinforces the idea that situational factors can elevate the risk of fraud when combined with weaknesses in oversight. The findings illustrate the need for vigilant monitoring and active oversight, reiterating Thakur

(2024) assertion that environments characterized by robust security measures and surveillance see lower crime rates.

The application of Routine Activity Theory necessitates a re-envisioning of regulatory compliance structures within Kenyan banks. Effective compliance mechanisms can act as capable guardians against fraud. By ensuring that banks adhere to recognized standards and regulations, the likelihood of routine activities leading to fraudulent acts can be diminished. However, regulations must be complemented by technological solutions capable of adapting to the evolving fraud landscape. For instance, the implementation of Artificial Intelligence (AI) systems for transaction monitoring can provide real-time oversight, swiftly identifying unusual patterns that may indicate fraudulent behavior (Bello & Olufemi, 2024).

Koehn (2019) found that economic pressures, such as high unemployment and income inequality, are key drivers of fraud in Kenya. These pressures are compounded by the study's variable, Organizational Culture, as a culture that tolerates unethical behavior can further motivate individuals to commit fraud. For example, employees who perceive that their colleagues are engaging in fraudulent activities without consequences may be more likely to do the same.

The swift integration of technological advancements in Kenyan commercial banks has resulted in new opportunities for fraudsters, particularly through digital banking platforms and mobile payment systems. A study by Gulyas and Kiss (2023) indicates that while these technologies enhance access to financial services, they also expose new vulnerabilities, including cyberattacks and identity theft. This situation highlights the critical need for robust internal control systems to safeguard against such threats. Additionally, Mochere (2020) found that many banks in Kenya lack the necessary resources and expertise to effectively monitor and prevent fraudulent activities. This deficiency is especially concerning given the rapid pace of technological change, which complicates banks' efforts to keep up with the evolving tactics employed by fraudsters.

However, staff training acts as a critical moderating factor in strengthening these fraud deterrence strategies. Employees who are well-trained in fraud detection techniques,

ethical banking practices, and compliance measures serve as capable guardians who deter fraudulent activities (Omondi & Wanjiru, 2022). Additionally, training ensures that employees are equipped to recognize and respond to emerging fraud schemes, thereby reducing vulnerabilities within banking institutions.

Routine Activity Theory offers a valuable framework for understanding how everyday banking practices and insufficient oversight can create opportunities for fraud. This study aims to leverage the theory to pinpoint routine activities that heighten the risk of fraud in Kenyan commercial banks and to suggest measures that enhance oversight and mitigate these risks. By addressing these situational elements, banks can substantially lower the chances of fraudulent occurrences. This insight will facilitate the development of targeted interventions that focus on specific vulnerabilities, promoting a comprehensive approach to fraud prevention within the banking sector. These strategic methods enable secure banking environments which build up the financial system's stability together with its integrity.

Routine Activity Theory (Cohen & Felson, 1979) shifts the focus from individual traits to situational factors, proposing that crime occurs when three elements align: a motivated offender, a suitable target, and a lack of capable guardianship. In the context of fraud in Kenyan banks, everyday banking activities, such as cash handling, loan approvals, and customer transactions, often lack sufficient oversight, making them attractive targets for fraud.

Routine Activity Theory connects directly to Objective iv, which examines the effect of technological advancements on the occurrence of fraud. Technological advancements such as AI-driven monitoring systems and real-time fraud detection act as capable guardians, reducing opportunities for fraud by providing continuous surveillance. Additionally, Objective v is relevant here, as staff training enhances guardianship by equipping employees with the skills to identify and respond to fraud, ensuring that they actively monitor transactions and detect fraudulent activity.

The theory also highlights the importance of situational factors in fraud prevention. Routine Activity Theory suggests that when routine activities are not adequately

supervised or when technology is underutilized, fraud risks increase. By integrating staff training with technological advancements, banks can address these vulnerabilities and reduce the opportunities for fraud.

2.3 Empirical Literature Review

This section of the study examined the existing literature on the factors influencing fraudulent practices within Kenyan commercial banks. It investigated the role of internal control systems in preventing or failing to detect fraudulent activities. The reviews also evaluate the impact of regulatory compliance on the occurrence of bank fraud, analyzing various compliance frameworks and their effectiveness. Furthermore, the influence of organizational culture on the development of fraudulent behaviors explored, identifying cultural elements that may either promote or discourage such practices. Finally, the section assessed the role of technological advancements in shaping fraud detection and prevention strategies, with a focus on the latest tools and their implications for security within the banking sector.

2.3.1 Internal Control Systems and Fraudulent Practices

Organizations that operate commercial banks need strong internal control systems to stop fraudulent activities. Internal control systems as defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) consist of frameworks that provide reasonable assurance about organizational success in achieving operational targets while complying with laws. These systems play a critical role in detecting and preventing fraudulent activities, protecting assets, and upholding the integrity of financial reporting (Igbojioyibo, 2024). However, while internal controls play a critical role, the effectiveness of these systems remains a subject of debate across different banking contexts, particularly in relation to how they combat fraudulent practices. This review aims to explore how internal controls function within commercial banks, focusing on their strengths, limitations, and relevance in reducing fraud.

Several studies have investigated the link between internal control systems and fraud prevention, presenting both complementary and contrasting findings. Ilugbusi et al. (2020) found that comprehensive risk assessments significantly reduced fraud in Nigerian banks, highlighting the importance of thorough risk management in fraud prevention. This aligns

with the findings of Chen and Elder (2021), who also emphasized the importance of strong monitoring and risk assessment mechanisms in U.S. banks to reduce fraud. Both studies underscore the role of robust risk management, but a key difference lies in their contextual application—the study by Chen and Elder was conducted in a technologically advanced banking system, which may not directly apply to Kenyan banks, where technological infrastructure is still developing. This contextual gap is important, as it calls for a tailored approach to implementing risk assessments in Kenyan banks, considering their relatively less advanced technological capabilities.

In contrast, Fernandhytia and Muslichah (2020) brought an additional layer by integrating the role of individual morality and ethics into the internal control framework. Their study suggested that strong internal controls need to be complemented by ethical training to act as a deterrent to fraud. This finding introduces a new dimension, emphasizing that fraud prevention is not only about technical control systems but also about fostering an ethical culture within the organization. However, Ilugbusi et al. (2020) did not address this cultural aspect and focused solely on the technical aspects of risk assessment. Moreover, Fernandhytia and Muslichah did not account for the impact of organizational size on the integration of ethical training, which could vary significantly between larger and smaller institutions. Smaller banks may find it more difficult to implement comprehensive ethical training programs compared to larger ones. This gap highlights the need for further research on how ethical training can be sustained in banks of different sizes, particularly in Kenyan banks, where resources and organizational scales can vary widely.

On the other hand, Ogola (2015) focused on management oversight in Kenyan banks, identifying poor segregation of duties and insufficient oversight as key weaknesses in internal controls. Ogola's findings highlight that poor management oversight creates opportunities for fraud, which is crucial for understanding why some internal controls fail. However, Ogola's study does not explore how regulatory changes over time impact the effectiveness of internal controls in Kenya. The evolving regulatory environment in Kenya suggests that regulations should be continuously adapted to mitigate fraud effectively. This gap presents an opportunity for further research into how regulatory frameworks influence the operation of internal controls, particularly in Kenyan banks.

A comparative study by Adegbite et al. (2021) and Molefe and Mkhize (2023) reinforced the importance of enforcing internal controls, particularly in the context of digital banking. Adegbite et al. focused on weak enforcement in Nigerian banks, showing that lax enforcement leads to increased fraud risks. Similarly, Molefe and Mkhize demonstrated that strong internal controls could reduce fraud by over 25%. Both studies support the view that enforcement is critical in fraud prevention, but they did not address the need to integrate cybersecurity measures into internal control frameworks. As digital banking and cybercrime become more prevalent, particularly in Kenya, integrating cybersecurity into internal controls is essential. This is a significant gap in the literature, as the current studies do not focus on how cybersecurity could enhance internal controls to defend against digital fraud.

Despite the valuable insights provided by previous studies on internal control systems and fraud prevention, several significant research gaps remain. First, there is limited exploration into how internal control systems function differently across various types of banks, such as large versus small institutions. The effectiveness of these systems may vary depending on the size, technological resources, and organizational capacity of the bank, a factor not adequately addressed in existing literature. Second, while ethical training is emphasized in fraud prevention, its long-term effectiveness in fostering a fraud-free culture within organizations, particularly in Kenyan banks, has not been thoroughly examined. There is a need to assess how ethical training can be sustained and continuously reinforced over time to create lasting cultural change. Third, the impact of evolving regulatory frameworks on the operational effectiveness of internal controls remains underexplored. As the regulatory environment in Kenya continues to evolve, there is a pressing need to understand how these changes influence the performance and adaptability of internal control systems in real-time. Additionally, the gap in technological infrastructure between more developed banking systems and those in Kenya highlights the need for further research on how internal controls and risk assessments can be effectively adapted in the Kenyan context, where technological infrastructure is still developing. Furthermore, while cybersecurity measures are acknowledged as critical in preventing fraud, few studies address their integration into internal control frameworks, especially with the rise of digital banking and cybercrime. This gap is particularly relevant

for Kenyan banks, where cybersecurity is becoming increasingly important as digital transactions proliferate. Finally, audit analytics and forensic accounting are commonly cited as effective fraud detection tools, but there is a lack of research on their limitations, particularly in detecting complex fraud schemes involving digital transactions. There is a clear need to explore how these tools can be adapted and refined to address the evolving fraud risks in the rapidly digitizing banking sector.

2.3.2 Regulatory Compliance and Fraudulent Practices

Regulatory compliance plays a vital role in maintaining the integrity and stability of banking systems, safeguarding against fraudulent activities, and protecting consumer interests. Compliance frameworks help banks navigate complex regulatory landscapes, ensuring operational integrity and legal conformity. Effective regulatory compliance not only prevents financial discrepancies but also upholds the reputation and trustworthiness of financial institutions. This structured approach is crucial in managing potential threats such as fraud and ensuring the long-term stability of the financial sector (Blair & Barbiani, 2019). While these frameworks are essential in fraud prevention, their effectiveness varies, especially with the increasing complexities brought about by emerging technologies and evolving financial crimes. As such, examining how regulatory compliance influences fraudulent practices is crucial to understanding how financial institutions can better safeguard themselves against these risks.

Several studies have explored the role of regulatory compliance in fraud prevention across different banking systems, providing insights that are applicable to the Kenyan context. Olojede et al. (2020) found that regulatory bodies helped minimize creative accounting but noted that weak enforcement mechanisms often produced inconsistent results. This highlights the need for stronger enforcement but does not explore how emerging technologies, such as blockchain or AI, could enhance compliance efforts and mitigate fraud risks in Kenyan banks. Otieno (2021) emphasized the importance of ethical compliance in reducing fraud, particularly in Kenyan professional accountants. While this study is relevant for the Kenyan banking sector, it did not assess the role of regulatory penalties in ensuring sustained ethical compliance, which is a critical element for long-term fraud prevention. Similarly, Wanjohi (2014) found that non-compliance with anti-

money laundering (AML) policies contributed to fraudulent activities in Kenyan banks but did not examine how risk-based regulatory approaches could further strengthen compliance. The gap here suggests that future research could explore how risk-based approaches can prioritize compliance efforts based on the likelihood and severity of risks, adapting to the changing fraud landscape in Kenyan banks.

Further studies, such as Clarke and Davison (2023), demonstrated that weak enforcement mechanisms in major international banks contributed to increased fraud. While their study advocated for stricter supervision and enhanced whistleblower protections, it did not address the challenges of implementing such measures in Kenyan banks, particularly between small and large institutions. This gap points to the need for research on how Kenyan banks, with varying resources, can balance effective compliance with available resources. Similarly, Osei and Boateng (2021) and Akpan and Okafor (2023) both highlighted gaps in enforcement within African banks, with Osei and Boateng focusing on Ghana and Akpan and Okafor on Nigeria. These studies align with findings from Waweru and Mutua (2022), who noted the inconsistent enforcement of CBK regulations in Kenya, which leaves the banks vulnerable to fraud. However, they do not explore how emerging technologies, such as blockchain or AI, could enhance regulatory compliance and fraud prevention in Kenyan banks. Kinyanjui (2023) proposed integrating blockchain technology to improve fraud prevention mechanisms in Kenyan banks but did not address the practical challenges of implementing such technology, such as lack of technical expertise and resistance from stakeholders. This presents a gap in understanding the challenges of adopting new technologies within Kenya's regulatory framework.

The potential of AI-driven technologies to improve regulatory compliance and fraud detection was explored by Oguejiofor et al. (2023), who suggested that data analytics and AI could streamline compliance processes, improve enforcement efficiency, and help regulatory bodies make informed decisions. However, Oguejiofor did not address how Kenyan banks can integrate data-driven approaches while ensuring compliance with CBK regulations. Similarly, Aziz and Andriansyah (2023) explored how AI enhances fraud detection and regulatory compliance by improving real-time decision-making. While their findings are relevant for Kenyan banks, they did not examine the ethical concerns and

risks associated with using AI in regulatory compliance, such as issues related to privacy, algorithm bias, or over-reliance on technology. The current study could address these concerns and explore how Kenyan banks can mitigate these challenges when integrating AI into their compliance systems.

While studies like Olojede et al. (2020) and Kinyanjui (2023) highlight the importance of regulatory frameworks, they do not explore how emerging technologies, such as blockchain or AI, can improve the effectiveness of regulatory compliance in preventing fraud. The integration of these technologies in Kenyan banks requires further investigation. Otieno (2021) emphasized the importance of ethical compliance, but there is a lack of research on the role of regulatory penalties in ensuring sustained ethical compliance in Kenyan commercial banks. Exploring how regulatory penalties can act as a deterrent to unethical behavior could provide valuable insights. Research such as Aziz and Andriansyah (2023) demonstrates the potential of AI in enhancing fraud detection, but the practical challenges of adopting these technologies in Kenyan banks remain unexplored. There is a need to investigate how Kenyan banks can overcome barriers, such as technical expertise, resource constraints, and stakeholder resistance, to successfully integrate these technologies. Wanjohi (2014) and Clarke and Davison (2023) highlighted compliance failures, but did not explore how risk-based approaches could strengthen compliance efforts in Kenyan banks. This is an important area for further research, especially as banks face increasingly sophisticated fraud risks.

2.3.3 Organizational Culture and Fraudulent Practices

Organizational culture plays a crucial role in shaping the ethical environment and operational integrity of banking institutions. A strong and ethical culture can greatly reduce the risk of fraud by fostering an atmosphere that encourages and rewards ethical behavior (Kasseem, 2022). On the other hand, a weak or toxic culture can contribute to higher instances of fraud and misconduct. Within banks, organizational culture affects employees' actions, decision-making, and adherence to internal controls and regulatory standards. Creating a culture of integrity and accountability is essential for preventing fraud and ensuring the long-term health and stability of financial institutions. Therefore,

understanding how organizational culture impacts fraud prevention is essential for Kenyan banks, where improving cultural aspects could enhance overall fraud mitigation strategies.

Several studies have examined how organizational culture affects fraud prevention, offering valuable insights into the dynamics between culture and fraudulent practices within financial institutions. Rashid et al. (2022) conducted a literature review and concluded that an ethical organizational culture, alongside strong internal controls, is crucial for fraud prevention. Their findings are relevant to Kenyan banks, emphasizing that fostering an ethical culture can strengthen fraud prevention strategies. However, they did not explore how employee engagement initiatives, such as participatory decision-making or team-building exercises, could further shape ethical behavior and reduce fraud. This is a research gap, as employee engagement plays a significant role in shaping the ethical culture within banks and warrants further investigation in the Kenyan context.

Naivasha (2021) investigated the role of strategic management at Kenya Commercial Bank, finding that a culture promoting ethical behavior and integrity among employees effectively reduced fraud. Similarly, Mwithi (2015) highlighted the importance of a culture centered on ethical practices and transparency for mitigating fraud in Kenyan banks. However, Naivasha's study did not assess the effectiveness of reward systems in reinforcing ethical behavior. This presents another gap, as incentives and rewards can significantly influence employees' commitment to upholding ethical standards. Further research should explore how reward systems can be integrated into the culture to reinforce ethical behavior and reduce fraud in Kenyan banks.

Jones and Patterson (2022) and Liu and Zhang (2023) found that banks with strong ethical cultures experienced fewer fraud incidents. These studies support the need for a robust ethical culture within Kenyan banks. However, they did not address the role of whistleblower protection policies in fostering such a culture. Whistleblower protection is critical for encouraging employees to report unethical behavior without fear of retaliation, a key area for research in Kenyan banks to reduce fraud. This gap is significant and should be explored in further studies.

In South Africa, Dlamini and Khoza (2022) emphasized the importance of ethical training and leadership accountability in curbing fraud. Their findings align with Jones and Patterson's work and suggest that ethical training is essential for fraud prevention. However, Dlamini and Khoza did not assess the long-term impact of ethical training on reducing fraud, leaving a gap in understanding the effectiveness of sustained cultural change over time. Research on the sustainability of ethical training in Kenyan banks is needed to evaluate its long-term effectiveness and how it can be integrated into continuous employee development.

Mwangi and Kimani (2023) found that Kenyan banks that foster integrity, transparency, and ethical behavior had lower fraud rates. This aligns with the objectives of the current study, emphasizing the role of ethical leadership and transparency in fraud prevention. However, it would be valuable to assess how these ethical training programs can be integrated with technological tools, ensuring their sustainability and relevance in the face of evolving fraud risks. This is particularly important as technology plays an increasing role in the banking sector.

Onyancha (2023) explored corporate governance and fraud prevention in Kenyan microfinance banks, finding that strong governance structures—such as independent boards and established codes of conduct—played a crucial role in reducing fraud. This is particularly relevant for Kenyan commercial banks, as it highlights the need to integrate governance frameworks with ethical standards. However, Onyancha did not explore how corporate governance frameworks can be adapted to address the challenges posed by the digital banking landscape. This gap is significant given the rapid growth of digital banking in Kenya, where emerging risks such as cybersecurity threats and online fraud require new governance models.

In the broader context, Al-Mamun et al. (2020) explored the relationship between corporate governance and fraud prevention across multiple jurisdictions. Their study found that an active, independent board and transparent reporting mechanisms are essential in mitigating fraud. However, they did not examine how cross-border regulatory differences affect corporate governance practices, which is an important aspect for Kenyan banks that operate within a globalized financial environment. This gap points to

the need for research on how Kenyan banks can align their governance structures with international best practices while remaining compliant with local regulations.

While studies such as Rashid et al. (2022) emphasize the importance of an ethical organizational culture, they do not explore how employee engagement initiatives, such as participatory decision-making or team-building exercises, can further shape the culture and reduce fraudulent activities. Additionally, Naivasha (2021) and Mwithi (2015) highlight the significance of fostering an ethical culture, but they do not assess the role of reward systems in reinforcing ethical behavior. Investigating these employee engagement initiatives and reward systems in Kenyan banks could offer new insights into how they can encourage ethical behavior and reduce fraud. While Jones and Patterson (2022) and Liu and Zhang (2023) emphasize the importance of ethical leadership, they do not address the role of whistleblower protection policies in fostering an ethical culture, a critical area for further research in the Kenyan context. Moreover, while Dlamini and Khoza (2022) emphasized the role of ethical training, they did not evaluate its long-term impact on fraud reduction, presenting a gap that could be explored further in the Kenyan banking sector. Lastly, while Onyancha (2023) discussed the importance of corporate governance in fraud mitigation, they did not consider how governance frameworks can be adapted to address digital banking challenges in Kenya, an area that warrants further investigation as digital banking continues to grow in the country.

2.3.4 Technological Advancements and Fraudulent Practices

Modern technological advancements have significantly transformed the banking sector by enhancing operational efficiency and enabling advanced customer interactions through new financial products. However, as financial institutions increasingly adopt digital technologies, they expose themselves to new security vulnerabilities, which are often exploited by cybercriminals. Cybercrimes, including identity theft and financial fraud, have become major concerns in the banking industry due to the expansion of digital banking platforms. To mitigate these risks, banks must integrate advanced technological solutions to safeguard their operations and protect customer data. Real-time transaction monitoring, powered by modern banking technologies, helps identify suspicious activities

quickly, enabling prompt responses to potential threats. This reduces the likelihood of fraud and strengthens the overall security infrastructure of banks.

Modern technological advancements have significantly transformed the banking sector, enhancing operational efficiency and enabling better customer interactions through new financial products. However, as banks increasingly adopt digital technologies, they are exposed to new vulnerabilities, which cybercriminals often exploit. Various studies have explored how technological advancements can help mitigate fraud risks, with Rai and Acharya (2021) finding that employee dissatisfaction, collusion between employees and customers, and inadequate information technology systems were key drivers of fraud in Nepalese banks. Their findings suggested the need for technological solutions, such as employee training and customer awareness initiatives, but Rai and Acharya's study did not explore how digital banking security protocols could be adapted to meet varying regulatory standards, a gap highly relevant to Kenyan banks, where regulatory frameworks are continuously evolving. Similarly, Hasham et al. (2019) explored how cybersecurity integration with fraud prevention strategies is crucial in managing emerging fraud risks. While their study highlighted the importance of advanced analytics and real-time monitoring systems, it did not examine how AI-powered systems could enhance the efficiency of fraud detection, representing a significant research gap for Kenyan banks facing increasing cyber threats.

Wanjohi (2014) and Palshikar (2002) also emphasized the importance of advanced security measures like firewalls, encryption, and data analytics to prevent fraud. However, neither study explored the role of biometric authentication in strengthening banking security, a gap that could be addressed by investigating how biometric technologies could complement traditional security systems to prevent fraud in Kenyan banks. Additionally, Tan and Wong (2023) and Sharma and Gupta (2022) found that AI-driven tools and blockchain-based methods were effective in reducing fraudulent transactions and improving financial security. However, both studies did not address the potential regulatory and ethical concerns related to the use of AI, such as privacy issues, algorithmic bias, and data protection. Given that Kenyan financial institutions are highly regulated,

understanding how to navigate these challenges while implementing AI and blockchain technologies in fraud detection is an area for further research.

In Zimbabwe, Ndlovu and Sibanda (2021) showed that biometric authentication significantly reduced mobile fraud, suggesting that such technologies could be adopted in Kenyan banks as well. Similarly, Okoro and Adewale (2023) analyzed fintech solutions for fraud prevention in Nigeria, emphasizing the importance of real-time monitoring systems. While both studies offer valuable insights, neither examined the effectiveness of combining two-factor authentication with biometric methods for a more comprehensive fraud prevention system. Exploring how these technologies can work together to provide multi-layered security in Kenyan banks would be an important research direction.

Further, Kariuki and Wanjiru (2023) and Mutua (2023) highlighted the need for improved cybersecurity infrastructure in Kenyan banks to combat rising fraud risks, but they did not explore the specific challenges these banks face when implementing advanced fraud detection systems. These challenges include resource limitations, technical expertise, and collaborative efforts between stakeholders. Addressing these barriers to the adoption of advanced digital fraud detection technologies should be a focal point for future research. Finally, Utami et al. (2020) discussed the need for stronger IT governance in preventing fraud, but their study did not consider how IT governance could be integrated with broader organizational strategies to create a more comprehensive fraud prevention framework in Kenyan banks. This is an essential gap, especially as banks continue to modernize their technological infrastructure.

While various studies have underscored the potential of AI, blockchain, and biometric systems to improve fraud detection and prevention, several research gaps remain. These include the need to explore how digital security protocols can be tailored to meet regulatory standards in Kenya, the integration of biometric authentication with other security systems, the ethical and regulatory challenges of implementing AI in fraud detection, and the barriers faced by Kenyan banks in adopting advanced cybersecurity technologies. Additionally, further research is needed on how to combine two-factor authentication with biometric systems to create a multi-layered approach to fraud

prevention and how IT governance can be integrated with organizational strategies to enhance fraud mitigation.

2.3.5 Moderating Effect of Staff Training on Fraudulent Practices

Staff training plays a vital role in moderating the relationship between internal control mechanisms and fraud prevention in commercial banks (Hamed, 2023). Banks that invest in continuous training programs for their employees are better equipped to enhance their staff's ability to detect fraud and comply with regulatory requirements. Well-trained employees possess the necessary skills to identify fraudulent activities swiftly, which strengthens internal control systems and improves the overall effectiveness of fraud mitigation strategies within the institution (Nwachukwu et al., 2024). However, existing research has not sufficiently examined how the effectiveness of training programs differs across various hierarchical levels within banks, which remains a crucial area to explore in order to better understand how to target fraud prevention efforts effectively.

Staff training is a crucial factor in moderating the relationship between internal control mechanisms and fraud prevention in banks (Hamed, 2023). Research consistently highlights the importance of well-trained employees in detecting fraudulent activities and complying with regulatory requirements, which strengthens fraud mitigation strategies and internal control systems (Nwachukwu et al., 2024). However, one major gap identified is the insufficient exploration of how the effectiveness of training differs across hierarchical levels within banks. While some studies have focused on overall training effectiveness, few have examined how training impacts employees at different levels, from frontline staff to senior management. Future research should explore how targeted training programs could improve fraud prevention efforts at each level, particularly as fraud detection responsibilities vary.

Several studies have examined the role of staff training in enhancing internal controls and regulatory compliance, but they offer varying insights into the sustainability and evolution of these programs. Shwedeh and Rwashdeh (2022) found that training employees on regulatory requirements and ethical standards significantly reduced fraud levels in banks. However, their study did not address how continuous training could remain effective in a fast-paced financial environment, especially with emerging fraud techniques. Rwashdeh's

findings align with those of Bao et al. (2022), who emphasized that technological advancements, such as AI and blockchain, require highly skilled employees to interpret system outputs effectively. However, unlike Shwedeh and Rwashdeh, Bao et al. pointed out a gap in adapting training to the rapid development of digital fraud prevention tools, such as AI-powered systems. This gap is critical for Kenyan banks, where technology is evolving quickly and staff must be equipped to handle new challenges. Thus, there is a clear need for further research on how Kenyan banks can ensure training programs integrate new technological advancements while staying relevant to emerging fraud threats.

A significant gap in the literature is the disparity in access to training resources across various sizes of financial institutions. Larger banks tend to have more financial resources and can implement comprehensive training initiatives, while smaller institutions often struggle to offer similar opportunities. Donnellan and Rutledge (2019) discussed the challenges faced by smaller banks in providing adequate fraud training, which creates a gap in fraud prevention efforts across the banking sector. This highlights the need for cost-effective training solutions that can be scaled to meet the needs of banks of all sizes. Moreover, while Anindya and Adhariani (2022) and Zuberi and Mzenzi (2019) emphasized the behavioral impact of training on employees' attitudes toward fraud prevention, there is limited research on how employee perceptions evolve with varying levels of training. Studies on how training affects employee motivation, personal ethics, and compliance could offer valuable insights into designing training modules that cater to different employee needs. This approach could improve the effectiveness of fraud prevention initiatives in Kenyan banks, where diverse employee backgrounds and varying training needs may exist.

Supriadi (2024) also suggested that the integration of digital tools such as AI into training programs is crucial, but he did not explore how digital literacy impacts the ability of employees to engage with these advanced technologies. Moreover, while some studies, such as Tan and Wong (2023), have highlighted the potential of AI in fraud detection, the question of how staff training can be tailored to new technological realities remains unexplored. Training programs must evolve not only to equip employees with technical

skills but also to ensure they are capable of adapting to new technological developments in fraud detection, a gap that needs attention in future research.

The psychological and motivational factors behind staff adherence to fraud prevention policies are often overlooked. Zuberi and Mzenzi (2019) found that personal ethics and compliance motivation significantly influence the effectiveness of fraud prevention. However, studies on the psychological impact of training on behavior remain sparse, especially regarding how behavioral training can be structured to enhance fraud detection. Understanding how employees' attitudes change with increased training can help shape training programs that are more effective at reducing fraudulent activities in Kenyan banks.

The review reveals several key research gaps that need to be addressed to enhance the moderating effect of staff training on fraud prevention in Kenyan banks. These include the need to explore how training programs can be tailored to different hierarchical levels, how training can be sustained and adapted to technological advancements, and the integration of digital tools in training. Additionally, further research is needed to understand how to provide cost-effective training solutions for smaller banks and how to address psychological and motivational factors in fraud prevention training. Examining these gaps will provide critical insights into how Kenyan banks can improve their fraud prevention strategies by developing more targeted and effective staff training programs.

2.4 Research Gap

Despite extensive research into the factors contributing to fraudulent activities in the banking sector, there remains a significant gap in understanding how these dynamics specifically unfold within Kenyan commercial banks. Previous studies, such as those by Ilugbusi et al. (2020), Fernandhytia and Muslichah (2020), Lourens (2021), and Riitho and Wanjala (2020), have primarily focused on different geographic regions or types of financial institutions. For example, A research by Ilugbusi et al. (2020) analyzed how Nigerian banks use internal control systems to prevent fraud through comprehensive risk assessment methods. Fernandhytia and Muslichah (2020) studied the relationship between Indonesian bank internal controls and personal morality and ethical values to determine their effects on accounting fraud risks. However, these studies do not specifically address

the unique factors at play in Kenyan banks, suggesting the need for research that considers the specific challenges and opportunities within Kenya's banking environment. However, these investigations do not consider the distinct regulatory environment and cultural influences impacting Kenyan commercial banks. Therefore, it is essential to contextualize these findings within Kenya to better understand how local conditions affect the efficacy of internal control systems in curtailing fraudulent practices.

Olojede et al. (2020), Otieno (2021), and Oguejiofor et al. (2023) carried out research on regulatory compliance's influence on fraudulent practices targeting Nigerian populations together with Kenyan county governments. These studies establish how appropriate regulatory structures alongside ethical standards can minimize fraudulent activity. These studies overlook the specific regulatory obstacles and compliance systems which belong to Kenyan commercial banks. The investigation evaluates how regulatory compliance affects the rate of bank fraud among Kenyan commercial institutions under consideration of the country's existing regulatory framework and enforcement methods.

Additionally, studies by Rashid et al. (2022), Onyancha (2023), and Al-Mamun et al. (2020) have emphasized the critical role of organizational culture in shaping fraudulent behaviors. These studies stress the importance of ethical corporate governance and the cultivation of a culture rooted in honesty and integrity as key measures to prevent fraud. However, they do not delve into how these cultural factors specifically manifest within Kenyan commercial banks. This research aims to address this gap by examining the organizational culture within Kenyan banks and its impact on fraudulent activities. By focusing on the unique cultural dynamics in Kenyan banks, this study seeks to offer a more nuanced understanding of how organizational culture influences fraud, ultimately providing more effective cultural interventions and policy recommendations tailored to the Kenyan banking sector.

Furthermore, research by Rai and Acharya (2021), Hasham et al. (2019), and Utami et al. (2020) has explored the role of technological advancements in fraud prevention, highlighting the importance of advanced technologies such as artificial intelligence and cybersecurity measures in enhancing fraud detection and prevention. However, these studies do not specifically address how these technological advancements are applied

within Kenyan commercial banks. This study seeks to bridge this gap by examining how technological innovations influence fraud occurrences in Kenyan banks, taking into account local technological infrastructure and adoption rates. This approach provided valuable insights and actionable recommendations for effectively utilizing technology to combat fraud in the Kenyan banking sector.



Table 2.1 Summary of Literature and Research Gaps

Author	Study Objective	Methodology	Findings	Research Gap	How the Gap(s) Were Addressed in This Study
Ilugbusi et al. (2020)	Investigate the impact of internal control systems on fraud prevention in Nigerian banks	Quantitative research using regression analyses on survey data from bank employees	Enhanced internal control systems, especially rigorous risk assessments, significantly reduce fraud	Focused on Nigerian banks; need for similar studies in Kenyan commercial banks to understand local internal control effectiveness	The study expands on Ilugbusi et al.'s work by focusing on Kenyan commercial banks , exploring the effectiveness of internal controls in the local context.
Fernandhytia & Muslichah (2020)	Explore the relationship between internal control systems, individual morality, and ethical values in Indonesian banks	Mixed-methods approach with surveys and interviews of bank employees and managers	Strong internal controls combined with high ethical standards significantly lower accounting fraud	Limited to Indonesian banks; need for research on how these dynamics play out in Kenyan commercial banks	This study investigates how ethical values and internal controls interact in Kenyan banks , filling the gap in the Kenyan context.
Lourens (2021)	Analyze the dual benefits of internal control systems in South African banks on financial performance and fraud management	Quantitative study surveying bank managers and auditors	Stringent internal controls significantly enhance financial stability and decrease fraud incidents	Specific to South African banks; need to assess the applicability of these findings to Kenyan commercial banks	The study applies Lourens' findings to the Kenyan banking sector , considering how local conditions might affect fraud management and financial performance.

Riitho & Wanjala (2020)	Examine the influence of internal control systems on fraud detection and prevention among Saccos in Kenya	Quantitative approach with Ordinary Least Squares Regression analysis of survey data	Well-implemented internal control components significantly mitigate fraud risk	Focused on Saccos; need to evaluate similar controls in Kenyan commercial banks	This research extends Riitho & Wanjala's findings by evaluating internal control systems specifically in Kenyan commercial banks , beyond Saccos.
Olojede et al. (2020)	Investigate the impact of regulatory agencies on creative accounting practices in Nigeria	Descriptive survey research with multi-stage sampling of 405 respondents	Regulatory agencies significantly curb creative accounting practices, though effectiveness varies	Nigerian context; need to explore regulatory compliance effectiveness in Kenyan commercial banks	The study examines how Kenyan regulatory bodies influence fraud prevention in commercial banks, addressing the gap in Kenyan regulatory compliance .
Otieno (2021)	Examine the effects of ethical compliance on professional accountants in selected county governments of Kenya	Qualitative methodologies including in-depth interviews and document analysis	High ethical compliance correlates with significant reduction in fraudulent activities	Focused on county governments; need to study ethical compliance in Kenyan commercial banks	The study shifts focus to Kenyan commercial banks , specifically analyzing how ethical compliance impacts fraud mitigation in banking .
Oguejiofor et al. (2023)	Review data-driven regulatory compliance in Nigeria	Review of literature and case studies	Data-driven approaches and AI significantly enhance compliance efforts amidst	Nigerian regulatory landscape; need for research on data-driven compliance in	This research extends Oguejiofor's review by investigating the role of AI and data analytics in Kenyan banks ,

			bureaucratic hurdles	Kenyan commercial banks	addressing the gap in local compliance .
Rashid et al. (2022)	Identify effective approaches to prevent corporate fraud through literature review	Review of peer-reviewed articles from 2003 to 2018	Strong internal controls, ethical corporate governance, and culture of honesty are vital in fraud prevention	Broad review; need for context-specific studies in Kenyan commercial banks	This study builds on Rashid et al.'s findings , applying them to Kenyan commercial banks , and offers context-specific recommendations.
Onyancha (2023)	Examine the effect of corporate governance on fraud mitigation among microfinance banks in Kenya	Descriptive research with surveys of 186 management employees from 14 microfinance banks	Effective corporate governance significantly contributes to fraud mitigation	Focused on microfinance banks; need to explore these dynamics in Kenyan commercial banks	This study broadens Onyancha's findings to include Kenyan commercial banks , considering the unique challenges of larger institutions.
Al-Mamun et al. (2020)	Examine the relationship between corporate governance and fraud prevention in financial institutions across jurisdictions	Mixed-method approach with qualitative and quantitative data	Strong corporate governance, active board, and internal controls prevent fraud	Cross-jurisdictional; need to apply findings to Kenyan commercial banks	The research applies cross-jurisdictional findings to Kenyan commercial banks , providing insights on aligning governance with local regulations .
Rai & Acharya (2021)	Explore causes and preventions of banking frauds in Nepal	Exploratory-descriptive research with a questionnaire	Significant causes of fraud include employee dissatisfaction, poor data	Nepalese context; need for similar studies in Kenyan commercial banks	This study applies the findings to Kenyan commercial banks , identifying local causes of fraud and effective

		based on fraud theories	management, and inadequate IT systems		prevention strategies in Kenya.
Hasham et al. (2019)	Discuss impact of cybersecurity on financial crime and fraud	Descriptive research analyzing cybersecurity threats and implications for financial institutions	Traditional approaches inadequate for evolving cyber threats; need for integrated cybersecurity and fraud prevention strategies	Broad international context; need for specific focus on Kenyan commercial banks	The study focuses on cybersecurity threats in Kenyan banks , specifically examining local digital fraud risks and security measures .
Utami et al. (2020)	Examine effect of IT governance, internal control, and organizational culture on fraud prevention in Indonesian banks	Quantitative research with partial least squares analysis	Internal control and organizational culture significantly affect early fraud prevention; IT governance impact less significant	Indonesian context; need for studies on IT governance and fraud prevention in Kenyan commercial banks	This study localizes IT governance and fraud prevention practices for Kenyan banks , addressing how Kenya's banking sector can enhance IT governance .

These research gaps emphasize the need for context-specific studies, particularly focusing on commercial banks in Kenya. It is crucial to understand how internal controls, regulatory compliance, organizational culture and technological advancements impact the occurrence of fraudulent practices within these banks.

2.5 Conceptual Framework

This section presents the independent and dependent variables, as well as the conceptual model relevant to the study. The conceptual model, depicted in Figure 2.1, illustrates the relationships among the variables under investigation. This research focuses on how internal control systems, regulatory compliance, organizational culture, and technological advancements (independent variables) impact the occurrence of fraudulent practices (dependent variable) in Kenyan commercial banks.

The dependent variable in this study is fraudulent practices, assessed based on the frequency and severity of reported fraud incidents and the effectiveness of mechanisms in detecting and preventing fraud. Understanding these practices is essential for developing strategies that strengthen the integrity and security of the banking sector. Internal controls play a vital role in preventing discrepancies that could lead to financial losses and harm to reputation. Effective internal controls provide a structured approach to monitoring operations, ensuring financial accuracy, and managing risks related to fraudulent activities (Coso, 2013).

Regulatory compliance refers to the adherence to laws, regulations, and ethical guidelines designed to protect against fraudulent activities and safeguard consumer interests. Proper regulatory compliance not only mitigates financial discrepancies but also maintains the reputation and trustworthiness of financial institutions by providing a structured method for managing potential threats (Blair & Barbiani, 2019).

Organizational culture significantly influences the ethical climate and operational integrity within banking institutions. A robust ethical culture can substantially reduce the risk of fraudulent activities by fostering an environment where ethical behavior is encouraged and rewarded. In contrast, a weak or toxic culture may lead to increased instances of fraud and misconduct. Establishing a culture of integrity and accountability is essential for preventing fraudulent practices and ensuring the overall health and sustainability of financial institutions (Kasseem, 2022).

Technological advancements have revolutionized the banking sector by offering benefits such as increased efficiency, improved customer service, and innovative financial

products. However, these advancements also introduce significant risks, particularly related to cybercrime and fraud. As banks become more digitized, they encounter new vulnerabilities that sophisticated cybercriminals can exploit. Therefore, implementing advanced technological solutions for fraud detection and prevention is critical for maintaining security and integrity within financial institutions. These technologies allow banks to monitor transactions in real-time, quickly detect suspicious activities, and respond effectively to potential threats, thereby minimizing the risk of fraud and improving overall operational security (Debbarma, 2023).

Staff training involves programs designed to help employees gain new skills and knowledge relevant to their roles, ultimately improving their performance and productivity (Noe, 2020). A moderator leads a group towards specific outcomes, not as a content expert, but as a facilitator of techniques, ensuring equal participation and maintaining neutrality. They guide participants, ask relevant questions, and manage discussions to avoid unproductive conflicts.

Skill development ensures participants achieve their learning goals, filling content gaps through trainer input, self-reflection, and knowledge exchange among participants. Skill development includes instilling practical skills to apply compliance knowledge in daily roles and nurturing critical thinking for ethical dilemmas. Technical training, facilitated by a moderator, should clearly link to employees' responsibilities and career progression (Gutterman, 2023).

Compliance training is designed to address specific regulatory and legal requirements pertinent to an organization, aiming to reduce the potential legal repercussions associated with non-compliance. This type of training helps prevent misconduct, ensures effective governance, and protects the organization from various risks.

The conceptual model shown in Figure 2.1 illustrates the expected impact of the independent variables internal control systems, regulatory compliance, organizational culture, and technological advancements on the dependent variable of fraudulent practices among employees in Kenyan commercial banks, with staff training acting as a moderating factor.

Independent Variables

Dependent Variable

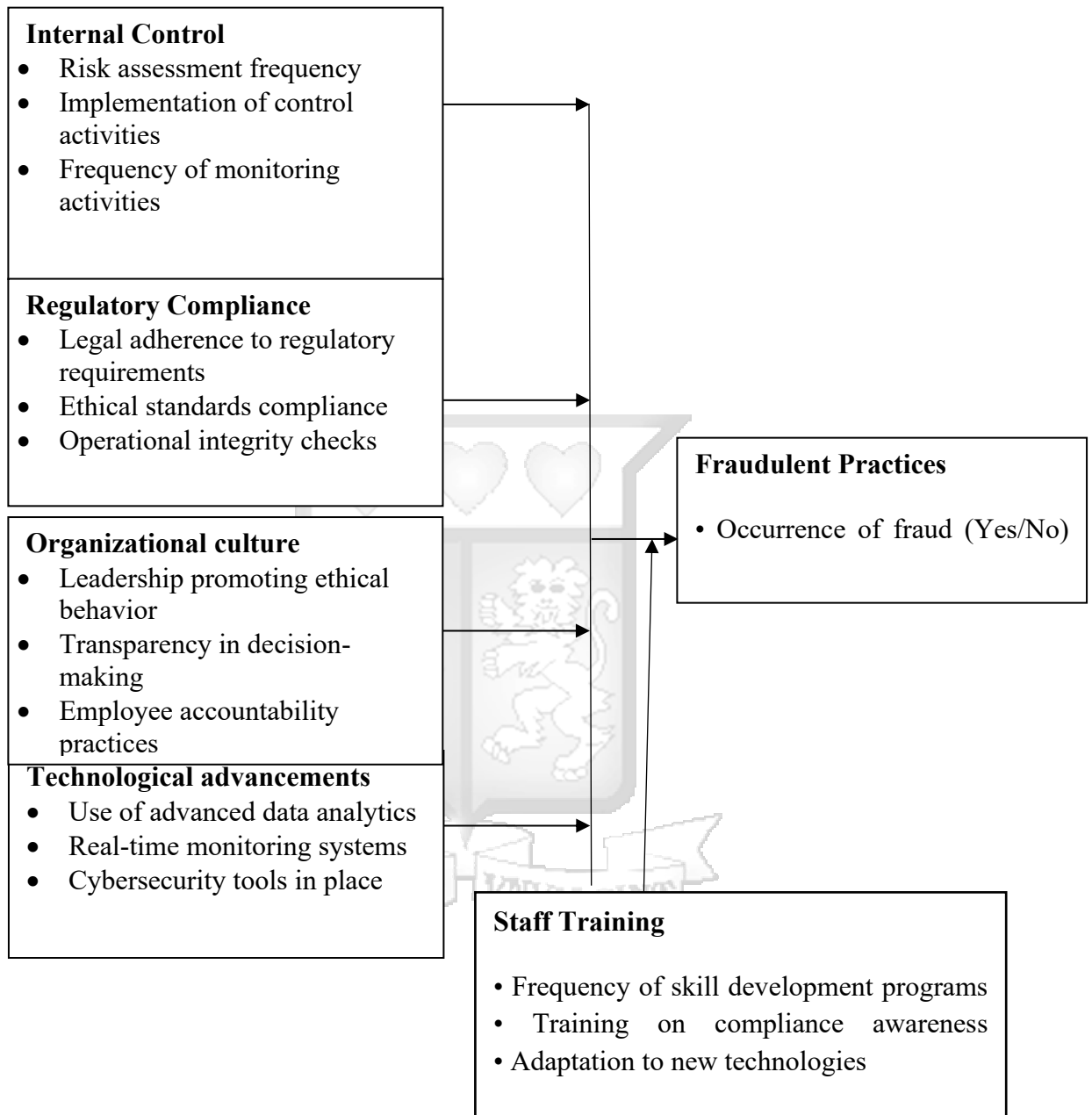
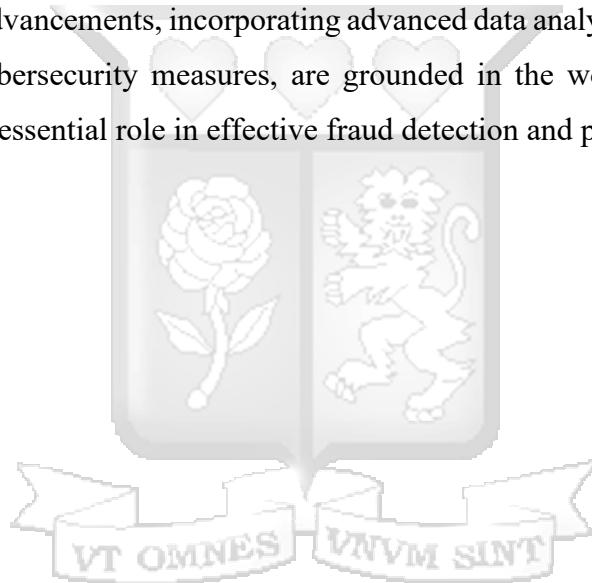


Figure 2.1 Conceptual Framework

The justification of the research variables for the current study on the determinants of fraudulent practices among employees in Kenyan commercial banks is as follows. Internal control systems, which include risk assessments, control activities, and continuous monitoring, are adopted from the COSO framework (2013), emphasizing their importance in preventing discrepancies and managing potential threats. Regulatory compliance, encompassing legal adherence, ethical standards, and operational integrity, is based on Blair and Barbiani (2019), highlighting its crucial role in maintaining the reputation and trustworthiness of financial institutions. Organizational culture, including ethical leadership, accountability, and integrity, is derived from Kasseem (2022), which underscores the importance of an ethical culture in mitigating fraudulent activities. Technological advancements, incorporating advanced data analytics, real-time monitoring systems, and cybersecurity measures, are grounded in the work of Debbarma (2023), illustrating their essential role in effective fraud detection and prevention.



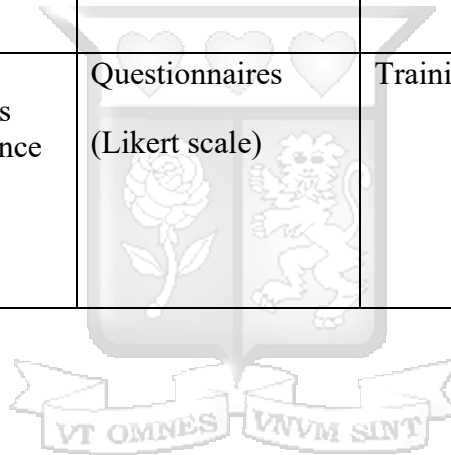
2.6 Operationalization of study variables

This section identifies the independent and dependent variables of the study.

Table 2.2: Operationalization of Variables

Variable	Indicators	Data Collection Method	Data Source	Data Analysis	References
Fraudulent Practices (Dependent Variable)	<ul style="list-style-type: none"> • Occurrence of fraud (Yes/No) 	Questionnaires, bank reports, fraud audit data	Fraud incident reports from banks CBK annual reports Audit summaries	Descriptive statistics Trend analysis Regression analysis	Central Bank of Kenya (2023), Audit Reports
Internal Control Systems (Independent Variable)	<ul style="list-style-type: none"> • Risk assessment frequency • Implementation of control activities • Frequency of monitoring activities 	Questionnaires (Likert scale)	Internal audit reports Employee responses	Correlation analysis Regression analysis	COSO (2013), Ilugbusi et al. (2020)
Regulatory Compliance (Independent Variable)	<ul style="list-style-type: none"> • Legal adherence to regulatory requirements • Ethical standards compliance • Operational integrity checks 	Questionnaires (Likert scale)	Bank compliance reports Regulatory filings	Regression analysis Comparative analysis	Blair & Barbiani (2019), Otieno (2021)
Organizational Culture	<ul style="list-style-type: none"> • Leadership promoting ethical behavior • Transparency in decision-making 	Questionnaires (Likert scale)	Employee responses	Regression analysis Descriptive statistics	Onyancha (2023), Rashid et al. (2022)

(Independent Variable)	<ul style="list-style-type: none"> • Employee accountability practices 				
Technological Advancements (Independent Variable)	<ul style="list-style-type: none"> • Use of advanced data analytics • Real-time monitoring systems • Cybersecurity tools in place 	Questionnaires (Likert scale)	IT system logs Technology adoption reports	Regression analysis Descriptive statistics	Hasham et al. (2019), Rai & Acharya (2021)
Staff Training (Moderating variable)	<ul style="list-style-type: none"> • Frequency of skill development programs • Training on compliance awareness • Adaptation to new technologies 	Questionnaires (Likert scale)	Training staff records	Regression analysis Descriptive statistics	Gutterman, (2023).



2.7 Chapter Summary

This chapter provides a summary of the theoretical and empirical literature review, outlining the conceptual framework for the study. It examines key theories and empirical findings related to the determinants of fraudulent practices among employees in Kenyan commercial banks. Theories such as the Fraud Triangle Theory, Institutional Theory, and Routine Activity Theory are explored, emphasizing the impact of internal control systems, regulatory compliance, organizational culture, and technological advancements on fraudulent behaviors. This chapter provided details about the research methodology which included research philosophy along with design and population and sampling methods and data collection and analysis techniques.



CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research methodology used to achieve the objectives of the study. It describes the different approaches applied, starting with the selection of the target population and extending to the ethical guidelines that governed the research process. Specifically, this chapter addressed the following components: research design, target population, sampling method, data collection instruments, data collection procedures, pilot study, reliability and validity assessments, data analysis techniques, and ethical considerations.

3.2 Research Philosophy

Saunders et al. (2019) stated that research philosophy is a system of beliefs and assumptions about knowledge development and reality which serve as the foundation of research. It offers a framework for how researchers perceive the world and approach their studies, influencing their choice of research methods, data collection, and analysis. Various research philosophies exist, each offering a distinct view on how knowledge is acquired and understood.

One widely used research philosophy is positivism, which assumes that reality is objective, observable, and can be empirically measured. Positivists rely on quantitative data and scientific methods to test hypotheses and establish general laws or patterns. This philosophy, rooted in the natural sciences, emphasizes objectivity and neutrality in research (Hammersley, 2019). However, interpretivism is concerned with the understanding of subjective meaning and experience of people. Interpretivists contend that reality is built socially so that we must study how people come to hear, and make sense, of their social world. This approach is often linked to qualitative research methods such as interviews and ethnography (Willis, 2007). Pragmatism, another research philosophy, emphasizes practical outcomes and problem-solving. Pragmatists prioritize the research question over strict adherence to a particular methodology, often integrating both qualitative and quantitative methods (Creswell & Creswell, 2017). Finally, realism recognizes the existence of an objective reality but acknowledges that our understanding

of it is shaped by social, cultural, and historical contexts. Critical realists, like Bhaskar (2008), argue that while reality exists independently of human perception, our knowledge of it is always mediated by social structures and processes.

The research philosophy applied in this study is positivist, which agreed that reality is objective, can be observed and described from an impartial way, without the researcher's bias or interpretation. Positivism holds that knowledge is derived from empirical evidence and logical analysis, based in observable phenomena, and by means of scientific methodology to formulate patterns and laws of the human behavior (Bryant, 1985).

By adopting a positivist approach, this research used structured methodologies to collect and analyze quantitative data to identify and measure the determinants of fraudulent practices among employees in Kenyan commercial banks. This is aligned with the objectives of the study as it allows for the study of relationships between variables with the use of statistical techniques so that the results are reliable and generalize (Hasan, 2016).

Furthermore, the positivist paradigm supports the use of standardized instruments, such as structured questionnaires, which help maintain objectivity and neutrality throughout the study. This methodological choice is in line with the principles of positivism, which advocate for replicable research findings and the establishment of universal laws applicable across similar contexts (Berkovich, 2018).

3.3 Research Design

This study adopted an explanatory research design, aligned with the positivist research philosophy, to explore how and why the moderator, independent, and dependent variables interact. The goal of explanatory research is to establish causal links between variables (Baskerville & Pries-Heje, 2010). Specifically, this research aims to investigate "the moderating effect of staff training on the relationship between the determinants of fraudulent practices among employees in Kenyan commercial banks," focusing not only on whether staff training influences fraudulent behavior but also on how it affects the relationship between the factors contributing to fraud and the actual fraudulent activities.

This approach is consistent with the primary objective of explanatory research, which seeks to uncover the underlying reasons for a phenomenon by examining the causes and interrelationships between variables. Through quantitative methods and statistical analysis, this research tested hypotheses and provided evidence-based explanations for the observed relationships. The methodology enabled a comprehensive understanding of how different factors contribute to fraudulent activities within Kenyan commercial banks.

3.4 Population

Population is defined as the group of individuals that contains the whole that share characteristics, which are important for a research study (Creswell and Creswell, 2017). The population in this research is all 38 licensed commercial banks in Kenya as defined by the Central Bank of Kenya. The unit of analysis for this study are these banks which are in turn the primary focus of the interested population.

The unit of observation were the managers working in four key departments of these banks: risk management, compliance, internal audit, and governance. Commercial Banks are licensed and regulated by the Central Bank of Kenya. In 2023 it accounted for 38 licensed commercial banks in Kenya; the number of commercial banks branches increased to 1,511 from 1,475 recorded in 2022. The adult population using banks in Kenya was around 44% in 2021. The study's sample was designed to provide estimates at national, rural/urban, and across all forty-seven counties. These managers directly oversee fraud prevention, risk assessment, compliance with regulatory frameworks, and implementing governance policies. Their roles align closely with the study variables internal controls, regulatory compliance, organizational culture, and technological advancements making them the ideal participants for this study.

Table 3.1 Target population

Categories	Target population
Risk management	38
Compliance	38
Internal audit	38
Governance	38

Total	152
-------	-----

3.5 Sampling

3.5.1 Sampling Frame

The sampling frame is a complete or representative list or representation of all units of the population, which are eligible to enter the study (Bryman, 2016). For the purpose of this research, the sampling frame comprises of the 38 licensed commercial banks in-scope in Kenya as captured in Central Bank of Kenya (Appendix IV). From the 38 banks, manager from the following departments: risk management, compliance, internal audit, and governance departments formed the sampling frame.

3.5.2 Sampling Technique

Since the total population is small and manageable, this study employed a census sampling method, which involves collecting data from every unit within the population. Census sampling is defined as a method that includes all population members, ensuring comprehensive coverage and eliminating the potential for sampling error (Loeb et al., 2017). It is particularly suitable for small or manageable populations where full participation can be achieved. In this study, the census method ensures that data is collected from all 38 commercial banks and the managers in the four relevant departments, resulting in complete and reliable data for analysis.

Census sampling is advantageous for this study because it provides a holistic view of fraud prevention practices across Kenyan banking. It ensures that no relevant perspectives are excluded, thus enhancing the validity and generalizability of the findings (Denscombe, 2014). Additionally, it aligns with the study's objectives of providing actionable recommendations for all licensed commercial banks. The sample distribution across departments is summarized in Table 3.2.

Table 3.2 Sample size distribution

Department	Sample Size per Bank	Total Sample Size
Risk Management	1	38

Compliance	1	38
Internal Audit	1	38
Governance	1	38
Total	4	152

The census approach ensures complete coverage of all licensed commercial banks and their key departments, providing robust data for analyzing the determinants of fraudulent practices. This method supports developing reliable, valid, and actionable insights for addressing fraud in the Kenyan banking sector.

3.6 Data Collection Methods

Data collection refers to an organized process of obtaining and measuring information from several sources to answer particular research questions, or test hypotheses, or to assess the outcome (Creswell and Creswell, 2017). There, the secondary data was collected from the structured questionnaires and standard instruments on which further consistency and reliability had been taken care of in the responses.

The use of structured questionnaires allows for the collection of quantifiable data, making statistical analysis and comparison possible. These standardized tools were carefully developed to capture relevant information about the variables being studied, ensuring that the data is both valid and reliable for the research. This method provided a thorough understanding of the factors that influence fraudulent activities among employees in Kenyan commercial banks. Structured questionnaires are widely recognized for capturing quantitative data in a clear and organized format, making them suitable for studies with large populations and standardized variables (Bryman, 2016).

The study variables were expressed through statements rated on a five-point Likert scale in the closed ended questions of the structured questionnaire of the same, so that the respondents can respond to how much they agree or disagree with those statements. This approach effectively captures perceptions, attitudes, and practices and facilitates statistical analysis of the gathered data (Boone & Boone, 2012). The questionnaire was utilized to

collect information on various study variables, including internal control systems, regulatory compliance, organizational culture, and technological advancements.

Each question was carefully crafted to align with the study's objectives, ensuring that it is relevant and consistent with the research problem. It measures with a five-point Likert scale scores from 'strongly disagree' to 'strongly agree.' For quantifying subjective perceptions and attitudes and for statistical analysis of the pattern and relationships in the data, this scale is very useful (Boone & Boone, 2012). This structured approach was meant to provide reliable and valid data as the gains that can be made through understanding the factors that influence fraudulent practice amongst Kenyan commercial bank employees.

3.7 Data Collection Procedure

The researcher shall begin the research process by writing to the university to have the letter of introduction and subsequently seeking receipt of a research permit from the National Commission for Science, Technology & Innovation (NACOSTI), then seeking authorization from a commercial bank. The researcher articulated the study's purpose and requested participation from the bank. Bank management was contacted to facilitate access to the relevant departments and identify the target respondent's managers in the risk management, compliance, internal audit, and governance departments. The structured questionnaires were distributed to the identified managers either in hard copy or electronically, depending on the respondents' preferences and the logistical considerations. Electronic distribution was conducted using secure online survey platforms to ensure data security and convenience for respondents. Hard copies were delivered where electronic distribution is not feasible. Respondents were given adequate time to complete the questionnaires, with follow-up reminders to ensure timely submission. The researcher oversees the entire process, offering clarification and support to respondents when needed. Honest and accurate responses were encouraged with the assuring of anonymity and confidentiality.

3.8 Data Analysis

After data collection is complete, the responses are coded systematically and analyzed using the Statistical Package for the Social Sciences (SPSS version 30). The appropriate

objectives of the study were addressed using both descriptive and inferential statistics as their analysis.

The data collected was summarized and organized by means of descriptive statistics. To reveal general trends and patterns within the dataset certain key measures were applied including means, standard deviations, frequencies, and percentages. For example, the mean scores summarized participants' levels of agreement with statements related to fraud prevention practices, while standard deviations indicated the variability in responses. Descriptive statistics also highlight departmental variations, shedding light on how fraud prevention practices differ across the risk management, compliance, internal audit, and governance functions (Kim et al., 2015).

Correlation analysis and Ordinal Logistic regression (OLR) was a part of inferential statistics. Ordinal Logistic Regression (OLR) is a statistical technique for predicting an ordinal dependent variable with one or many independent variables (Grilli & Rampichini, 2021). An ordinal variable has ordered categories where the intervals between the categories are not precisely defined. OLR models the cumulative probabilities of an observation falling into or below a particular category.

A **binary logit regression model** is used to model situations where the dependent variable is binary or dichotomous in nature. This type of regression analysis predicts the probability of one of two possible outcomes, typically coded as 0 or 1. It is commonly used when the outcome of interest has only two categories, such as whether or not an event occurs, or in the context of fraud detection, whether a fraud case is detected or not.

In the case of fraudulent practices among employees in Kenyan commercial banks, the dependent variable (Y) would be **binary** representing whether or not fraud has occurred. The two categories could be defined as:

Y = 1: Fraudulent practices have occurred (fraud detected).

Y = 0: Fraudulent practices have not occurred (no fraud detected).

The purpose of the binary logit regression model is to estimate the likelihood or probability of an employee engaging in fraudulent activities, based on a set of independent variables that are believed to influence this probability.

Logistic Regression Equation

The binary logit regression equation is represented as follows:

$$\log \frac{P(Y=1)}{1-P(Y=1)} = \alpha + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 Z$$

Where:

$P(Y=1)$ is the probability of the dependent variable (fraudulent practices) being equal to 1 (fraud detected).

α is the intercept of the model.

X_1 = Internal Control

X_2 = Regulatory Compliance

X_3 = Organizational culture

X_4 = Technological Advancements

Z = Moderator (staff training)

$\beta_1, \beta_2, \beta_3, \beta_4, \beta_5$ are the regression coefficients to be estimated.

In this model, the equation calculates the log odds of the event occurring (fraud detection). The log odds are derived from the natural logarithm of the odds ratio, which compares the probability of the event happening to the probability of it not happening. The coefficients $\beta_1, \beta_2, \beta_3, \beta_4,$ and β_5 reflect how much the log odds of fraud detection change when each independent variable increases by one unit, assuming all other variables remain constant.

On fraudulent practices among employees in Kenyan commercial banks, the binary logit regression model would be applied to examine how the factors of internal control, regulatory compliance, organizational culture, technological advancements, and staff training (moderator) influence the likelihood of fraudulent activities occurring. This model would allow the researcher to estimate the probability of fraud detection (or lack thereof) based on the presence or absence of these factors.

The regression coefficients, once estimated, would tell:

The direction and strength of the relationship between each independent variable and the likelihood of fraud (whether better internal controls or stronger regulatory compliance reduce the likelihood of fraud).

In this study, hierarchical logistic regression can be particularly useful for evaluating the moderating effect of staff training. Initially, the model can include the main effects of internal control, regulatory compliance, organizational culture, and technological advancements to see how these predict fraud likelihood. Subsequently, staff training and interaction terms (e.g., staff training \times internal control) can be added to the model in the next step.

This stepwise approach enables the researcher to determine whether adding staff training significantly improves the model's ability to predict fraudulent practices. It also reveals whether staff training changes (moderates) the strength or direction of the relationship between the main predictors and fraud occurrence. Such moderation analysis is crucial for understanding how enhancing employee skills and awareness through training may strengthen or weaken the impact of fraud prevention factors.

Hierarchical regression is a statistical method that allows researchers to enter independent variables into a regression model in sequential blocks, based on theoretical rationale or empirical evidence (Cohen, Cohen, West, & Aiken, 2013). This technique helps in evaluating how much additional variance in the dependent variable is explained by a new set of predictors after accounting for variables already in the model. It is especially useful for testing moderation effects, where a moderator variable might change the strength or direction of the relationship between independent and dependent variables (Baron & Kenny, 1986).

For example, in studying fraudulent practices among employees in Kenyan commercial banks, researchers might first include core predictors such as internal control systems, regulatory compliance, organizational culture, and technological advancements. Subsequently, staff training can be added as a moderator variable to assess whether it enhances the predictive power of these determinants (Hayes, 2017). The change in explained variance between steps indicates the moderating role of staff training.

For example, in a study examining fraudulent practices among employees in Kenyan commercial banks, the researcher might first enter the key determinants such as internal control, regulatory compliance, organizational culture, and technological advancements

into the regression model. Then, in a second step, staff training as a moderator variable can be added. This enables the researcher to see how much staff training uniquely contributes to predicting fraudulent behavior beyond the core predictors. By comparing the explained variance (R^2) between models, the impact of staff training on the relationship between fraud determinants and fraud occurrence can be empirically evaluated.

3.8.1 Diagnostic Tests

When employing Ordinal Logistic Regression (OLR), the researcher takes into account several key assumptions. The first condition for ordinal scale arbitrary ordinal regression is the need to measure the dependent variable on an ordinal scale. Secondly, the independent variables could be continuous, categorical or ordinal.

It is also important that there is no multicollinearity among the independent variables: they should not have correlations among them higher than what you wish a relationship to be. Finally, we make the assumption that each independent variable has a proportional effect on each cumulative split of the ordinal dependent variable.

3.9 Research Quality

A pilot study involved approximately 10% of the total sample size, translating to 15 managers from the commercial banks' risk management, compliance, internal audit, and governance departments. All respondents of the pilot study were not participants of the main study. The structured questionnaire needed to be made more clear, reliable and valid, thus the pilot study was an essential preparatory step toward refining the structured questionnaire. A pilot study enables the feasibility testing of the research instrument, potential challenges to be discovered and the research instrument strengthened (Saunders et al., 2019).

3.9.1 Validity of Research Instruments

Validity can be defined as the extent to which the questionnaire measures what it is meant to measure. To ensure content validity, subject matter experts, including supervisors and experienced professionals in the banking sector, reviewed the research instrument to confirm that the questions adequately cover the study variables. Additionally, feedback

obtained from pilot participants guided improvements to ensure the instrument is comprehensive and relevant (Heale & Twycross, 2015).

3.9.2 Reliability of Research Instruments

In contrast, the reliability of the research instrument assesses the consistency by which the research instrument produces stable results. Cronbach's Alpha was used to analyze the responses of the pilot study responses on internal consistency. According to Taber (2018), a Cronbach's Alpha value of 0.7 and above was shown as indicative of acceptable reliability and values below this threshold was due to revamping of specific questionnaire items.

3.10 Ethical Considerations

Ethical considerations are crucial for conducting research with integrity, fairness, and respect for all participants. Every stage of the research process in this study, from data collection to findings presentation was shaped by the ethical guidelines. Participants were given any information relating to the study, including the purpose of the study, who they were involving, how the collected data was used, etc. prior to data collection. All respondents were informed of consent and if they have a direct understanding of the objectives, procedures of the study and the rights of the participants. This includes providing participants with an introductory letter that outlines the study's purpose, timeline, and expected outcomes. In addition, the letter pointed out that participation is voluntary and participants may withdraw from the study at any time with no consequences.

Confidentiality and anonymity were prioritized throughout the research. The questionnaire was designed to omit identifying information such as names, contact details, or other personal identifiers. Instead, the focus was on general demographic information such as age, gender, and department. All collected data was securely stored on my password protected device and was only accessible by the researcher. This protects the participant's privacy. The research presented the findings in aggregate for the reasons of not being able to link individual responses to participants.

Additionally, the researcher sought the necessary approvals from institutional and regulatory bodies to ensure ethical compliance. This process includes obtaining ethical clearance and an introduction letter from the researcher's academic institution. Strathmore University's Ethical Review Board also approved and the National Commission for Science, Technology and Innovation (NACOSTI) a research permit. These approvals ensured that the study complies with established ethical standards and regulatory requirements.

3.11 Chapter Summary

This chapter has outlined the research methodology that guided the study. It introduced positivist philosophy, emphasizing objectivity and empirical analysis, and proposed a descriptive research design to examine fraudulent practices among employees in Kenyan commercial banks. The population consisted of all 38 licensed commercial banks, with managers from four key departments risk management, compliance, internal audit, and governance as the observation unit. Census sampling was employed, targeting 152 respondents. Data were gathered using structured questionnaires featuring a five-point Likert scale and analyzed with SPSS for both descriptive and inferential statistics, including correlation and Ordinal Logistic Regression (OLR). Diagnostic tests were conducted to verify the validity of the regression model. Ethical considerations, including obtaining informed consent, ensuring confidentiality, and adhering to regulatory compliance, were followed throughout the study.

CHAPTER FOUR

PRESENTATION OF FINDINGS

4.0 Presentation of Findings

The research analysis and findings are presented in this chapter within the framework of established research methodology. The research examined how staff training serves as a moderating force that alters the connection between influencing factors which lead to employee fraud within Kenyan commercial banks. Descriptive statistics such as frequency and mean were used in the analysis

4.1 Response Rate

Study findings in Table 4.1 showed the response rate for the respondents in the survey conducted, questionnaires were distributed to 152 respondents, only 139 were returned, resulting in a response rate of 91.40%, which is considered high. The non-response rate was approximately 8.60%, with 13 questionnaires not returned.

Table 4.1 Response Rate

Responses	Frequency	Percentages
Questionnaires Responded	139	91.40
Questionnaires Not responded	13	8.60
Total	152	100

4.2 Pilot Study Results

The study performed a pilot test to verify both the reliability and validity qualities of its research instrument.

4.2.1 Reliability Test

The pilot study results of internal consistency reliability are presented in the table above. Table 4.2.

Table 4.2 Reliability Test

Variables	Cronbach's	N of Items
Internal control system	.826	7

Regulatory compliances	.710	7
Organizational culture	.746	7
Technological Advancement	.765	7
Staff Training	.768	7

Table 4.2 displays Cronbach's Alpha values alongside the number of items that measure different factors. Researchers employ Cronbach's Alpha to determine how consistent survey or questionnaire items function as an internal measurement system for reliability. The 'Internal control system' scale demonstrates an alpha value of .826 through 7 survey items. The questions which measure internal control system exhibit consistent features thus demonstrating high reliability levels.

Secondly, regulatory compliances showed a Cronbach's Alpha of .710, with 7 items. Thirdly, the organizational culture has a Cronbach's Alpha of 0.746, based on 7 items. Additionally, the technological Advancement is measured with a Cronbach's Alpha of 0.765 over 7 items. This high reliability indicates that the items assessing the Technological Advancement are consistent. Staff training had a Cronbach's Alpha of 0.768 over 7 items.

4.3 Demographic information

The study includes consideration of individual characteristics to both supply general data on respondents and enable the researcher to understand results. Here, the variables include the highest levels of education, job position, employment type, bank tier, gender and age range.

4.3.1 Gender of the Respondents

Table 4.3 indicates that among the respondents male participants accounted for 51.8% while female participants accounted for 48.2%. Male participants accounted for more than half of the total surveyed respondents. The research indicates that male respondents make up the significant portion of the study but female participants join them with equal numbers. The addition of male and female intellectual contributions will bring better results for the company.

Table 4.3 Gender of the Respondents

Gender	Frequency	Percentage
Male	72	51.8
Female	67	48.2
Total	139	100.0

4.3.2 Age Bracket of the Respondents

The research purpose was to identify the age group that participants belonged to. Table 4.4 presented the study results.

Table 4.4 Age Brackets of the Respondents

	Frequency	Percent
18-25 Years	19	13.7
26-35 Years	54	38.8
36-45 Years	39	28.1
46-55 Years	16	11.5
Above 56	11	7.9
Total	139	100.0

From the results, majority of the respondent 54(38.8%) were aged between 26-35 years. Additionally, 39(28.8%) of the respondent had an age bracket of 36-45 years and 19(13.7%) had an age bracket of 18-25 years while 16(11.5%) had an age bracket of 46-55 years of age and finally 11(7.9%) were above 56 years of age.

4.3.3 Education Level of the Respondents

The researcher also assesses the education level of the respondent. From the result, it indicates that 23(16.5%) had a PhD, 17(22.2%) had master's degree while majority of the respondent 53(38.1%) had a bachelor's degree and finally 46(33.1%) had a diploma level of education. Table 4.5 presents the study results.

Table 4.5 Education Level of the Respondent

Education level	Frequency	Percent
Diploma	46	33.1
Bachelor's degree	53	38.1
Master's Degree	17	12.2
PhD	23	16.5
Total	139	100.0

4.3.4 Job position of the Respondents

The researcher, however, aimed to ascertain the job position of the respondents. The study findings are illustrated in Table 4.6.

Table 4.6 Job Position of the Respondents

Job Position	Frequency	Percent
Risk Manager	52	37.4
Compliance officer	34	24.5
Internal Auditor	31	22.3
Governance Manager	22	15.8
Total	139	100.0

Table 4.6 showed that 52(37.4%) of the respondents indicated that they were working as risk managers, 34(24.5%) indicated that they were working as compliance officers, 31(22.3%) were working as internal auditors. Additionally, 22(15.8%) were governance managers. This implies that majority of respondents were employed in roles directly related to risk management and compliance, thus representing the significant representation of professionals engaged in core governance, risk, and control functions within their organizations.

4.3.5 Employment Type of the Respondents

The researcher also sought to establish the type of employment of the respondent. Table 4.7 presents the study results.

Table 4.7 Employment Type of the Respondents

	Frequency	Percent
Permanent	54	38.8
Contract	44	31.7
Temporary	41	29.5
Total	139	100.0

Study findings in Table 4.7 showed that majority of the respondent 54(38.8%) were employed permanently, 44(31.1%) were employed on a contract term and finally 41(29.5%) were employed on a temporary term. This implies that a significant proportion of the respondents held permanent employment positions, suggesting a stable workforce structure within the organizations, although a considerable number were also engaged on contract and temporary terms, indicating some level of employment flexibility.

4.3.6 Years of Working in the Banking Sector

The study also sought to establish the years of working in the banking sector of the respondents. Table 4.8 presents the study results.

Table 4.8 Years of Working in the Banking Sector

Years of Working	Frequency	Percent
Below 1 year	14	10.1
1 - 3 years	41	29.5
4 - 7 years	11	7.9
8 - 10 years	24	17.3
Over 10 years	49	35.3
Total	139	100.0

Findings indicates that, majority of the respondent 49(35.3%) had over 10 years of working in the banking sector. Also, 41(29.5%) of the respondent had had 1 – 3 years of working in the banking sector and 24(17.3%) had an experience of 8 to 10 years of working in the banking sector while 11(7.9%) had an experience of 4 to 7 years of working in the banking sector and finally 14(10.1%) an experience of less than 1 year of working in the banking sector.

4.3.7 Bank Tier Number of the Respondents

The researcher also sought to establish the bank tier number of the respondent. Table 4.9 presents the study results.

Table 4.9 Bank Tier Number of the Respondents

Bank Tier Number	Frequency	Percent
Tier 1 (Large Bank)	45	32.4
Tier 2 (Medium Bank)	52	37.4
Tier 3 (Small Bank)	42	30.2
Total	139	100.0

Study findings in Table 4.9 indicated that majority of the respondent 52(37.4%) were in medium banks (Tier 2), 45(32.4%) were in large bank (Tier 2) and finally 42(30.2%) were in small bank (Tier 3). This implies that the majority of respondents work in medium-sized banks (Tier 2), followed by large banks (Tier 1) and small banks (Tier 3). The distribution suggests that the study primarily captures the views of employees from medium-sized institutions, with a relatively smaller representation from large and small banks.

4.4 Descriptive Analysis

In this study, descriptive statistics were utilized to analyses both the independent and dependent variables. The examination comprises of measures such as the mean, frequencies, percentages, and standard deviation. A 5-point Likert scale was employed, with SD representing strongly disagree, D for disagree, N for neutral, A for agree, and SA for strongly agree, as shown in the following results.

4.4.1 Descriptive statistics Findings for Internal Control Systems

The first objective of the study was to assess the effect of internal control systems on the occurrence of fraudulent practices among employees in Kenyan commercial banks. The study results are presented in Table 4.10.

Table 4.10 Descriptive statistics Findings for Internal Control Systems

Statement	N	Minimum	Maximum	Mean	Stdv
1. The bank has a whistleblowing mechanism that helps in reporting fraudulent activities	139	1.00	5.00	3.70	1.23
2. The bank has effective internal control systems that prevent fraudulent activities.	139	1.00	5.00	3.81	1.28
3. Regular risk assessments are conducted to identify fraud risks.	139	1.00	5.00	3.71	1.25
4. There are clear policies and procedures in place to mitigate fraud.	139	1.00	5.00	3.68	1.36
5. Employee roles and responsibilities are well defined to prevent unauthorized transactions.	139	1.00	5.00	3.67	1.35
6. The internal audit department effectively monitors fraud risks and irregularities.	139	1.00	5.00	3.66	1.40
7. Internal control measures are regularly reviewed and updated to address emerging fraud risks.	139	1.00	5.00	3.77	1.30

$$\text{Percentage score for mean} = \frac{\text{Mean} - \text{Minimum}}{\text{Maximum} - \text{Minimum}} * 100$$

This formula calculates the percentage of the mean relative to the possible range of scores (from minimum to maximum). Mean: The average score obtained for each statement.

Minimum: The lowest possible score (in this case, 1.00). Maximum: The highest possible score (in this case, 5.00).

Table 4.10 reveals that the bank has established a whistleblowing mechanism as shown by the minimum rating of 1.00 and the maximum rating of 5.00. Data shows that the group of respondents expressed two completely different opinions. Plenty of bank employees demonstrate moderate approval of this whistleblowing mechanism since they scored it 3.70. This translates to 67.5% agreement suggesting that, on average, employees believe there is a moderately effective whistleblowing mechanism in place, but there is room for improvement. The standard deviation value of 1.23 points to an acceptable distribution of opinions since some people had different views about the bank's whistleblowing system's effectiveness. The study findings agreed with Hasan et al. (2022), who noted that banking fraud in Indonesia accounts for 41%, which is higher compared to other sectors. This is an important factor for the government and banking stakeholders to consider.

Table 4.10 also revealed that the bank maintains effective internal control systems that stop fraudulent activities according to participant responses which fell between 1.00 to 5.00. The measured scale demonstrates that different responses from the survey participants existed. Agreement among respondents was moderate since their mean score of 3.81 corresponded to 70.25% meaning the average response indicates a positive view of the effectiveness of internal control systems, though it is still not at the highest possible level. Some changes in observations emerge from the standard deviation of 1.28 because most people believe in internal control system effectiveness while several respondents remain skeptical. The research outcomes match Rashid (2022) who discovered that an internal control audit system remains critical for fraud prevention.

Risk assessments for fraud risks occur regularly at the bank based on responses ranging from 1.00 to 5.00 according to Table 4.10. The spread of responses shows widespread perspectives that started as strongly conflicting and went all the way to strong endorsement. An agreement of 67.75% about the issue can be inferred from a mean score of 3.71 on the survey scale. This implies that employees believe that risk assessments are conducted regularly but with some reservations about their effectiveness or frequency. The 1.25 standard deviation indicates that some respondents were uncertain about the

acknowledgment of the practice along with the majority of participants who understood its existence. Hashim Salleh Shuhaimi and Ismail (2020) reported similar results showing the existence of high fraud risks in state-controlled organizations that work with several government departments and private entities through procurement arrangements although they follow standard operating procedures and rules.

Further, the study indicates that the bank maintains a set of precise policies which fight fraud because respondents scored between 1.00 to 5.00. Multiple opinions exist within this scale of measurement. The results show participants agreed moderately since the mean score equaled 3.68 which corresponded to 67% suggesting that while policies and procedures are in place, employees may not fully perceive them as strongly mitigating fraud risks. This considerable variability within the standard deviation of 1.36 demonstrates that participants hold diverse opinions about whether people understand or support policies to prevent bank fraud. The study confirms the research by Onyango (2022) by showing that a zero-tolerance anti-fraud plan with an independent fraud reporting system alongside a comprehensive macro policy effectively protects against and responds to fraud acts. Real consequences that accompany a fraud reporting system encourage workers to submit more fraud cases to law enforcement.

Findings also demonstrates that the organization clearly defines employee duties for unauthorized transaction prevention through data ranging from 1.00 to 5.00. Multiple opinions exist across the studied sample based on this wide rate of response scores. The surveyed group demonstrated moderate agreement toward this topic by averaging a score of 3.67 corresponding to 66.75% agreement indicating that employees seem to feel that roles and responsibilities are defined, but there might be some ambiguity or gaps in clarity for fraud prevention. The 1.35 standard deviation value demonstrates considerable dispersion in how staff views role definition clarity and responsible communication. The study's findings are consistent with Wronka's (2022) research, which identified that crypto assets, due to their ease of electronic storage and transfer, present a significant risk of money laundering. As a result, their inclusion in the fifth AMLD was an essential action taken by European lawmakers.

The internal audit department monitors fraud risks and irregularities effectively according to Table 4.10 where responses scale from 1.00 to 5.00. The survey participants displayed varying levels of agreement about the topic. A 66.5% agreement exists between respondents as indicated by the 3.66 mean score. This implies that the internal audit department is perceived to be moderately effective in monitoring fraud, but improvements might be necessary for more proactive detection. A wide distribution of opinions relating to the bank-wide internal audit effectiveness is reflected by the 1.40 standard deviation value. The study results match the research outcomes from Kashona (2019) that showed internal audit standards are not being properly followed as well as auditing lacks objectivity because auditors depend on their employers and lack proper skills and the internal audit division does not receive enough support.

Review and updating of internal control measures to tackle emerging fraud risks was a practice through participant responses that ranged from 1.00 to 5.00. A wide range of viewpoints exists between the participants. The survey showed that 69.25% of respondents agreed with a score of 3.77 that the bank updates its internal controls to adapt to new risks. Employees believe that internal control measures are reviewed and updated regularly, indicating a moderate but positive approach to addressing emerging fraud risks. A standard deviation of 1.30 indicates varied understanding between respondents about internal control updates as well as awareness of these changes. The study's findings are consistent with the research conducted by Rahman, Hamzah, Jamaluddin, and Aziz (2019), which argues that SLR has been instrumental in identifying key players in the field, understanding their contributions, and revealing the future directions of internal control studies.

The percentage scores reflect a moderate-to-high level of agreement regarding the effectiveness of internal controls in fraud prevention within the bank, with room for improvement in several areas. The highest scores are observed in the effectiveness of internal control systems and the regular review of controls, suggesting that the bank has implemented some strong measures but still has areas to address, such as clearer role definitions, enhanced audit functions, and stronger whistleblowing mechanisms.

4.4.2 Descriptive Statistics Findings for Regulatory Compliance

The second objective of the study was to investigate the effect of regulatory compliance on the occurrence of fraud in Kenyan commercial banks. The findings of the study are presented in Table 4.11.

Table 4.11 Descriptive Statistics Findings for Regulatory Compliance

Statement	N	Minimum	Maximum	Mean	Stdv
1. The bank complies with all regulatory requirements related to fraud prevention.	139	1.00	5.00	3.64	1.33
2. Regulatory bodies conduct frequent audits and inspections to ensure compliance.	139	1.00	5.00	3.72	1.26
3. Employees are well trained on compliance policies related to fraud prevention.	139	1.00	5.00	3.72	1.34
4. Regulatory penalties are a strong deterrent against fraudulent practices.	139	1.00	5.00	3.82	1.19
5. The bank collaborates with regulators to enhance fraud detection and reporting.	139	1.00	5.00	3.86	1.16
6. The bank promptly addresses audit recommendations from regulatory bodies.	139	1.00	5.00	3.73	1.30
7. Compliance officers actively monitor and enforce fraud prevention policies.	139	1.00	5.00	3.81	1.26

$$\text{Percentage score for mean} = \frac{\text{Mean} - \text{Minimum}}{\text{Maximum} - \text{Minimum}} * 100$$

The study results in Table 4.11 showed that the bank complies with all regulatory requirements related to fraud prevention with a minimum of 1.00 and a maximum of 5.00, indicating that the respondents disagreed, others agreed. The mean was 3.64, which (66.0%) shows that employees view compliance with regulatory requirements as

moderately effective, indicating a need for greater effort in adhering to all regulatory standards for fraud prevention. The standard deviation of 1.33 suggests a fair amount of variability in responses, meaning not all respondents had the same view on bank compliance with all regulatory requirements related to fraud prevention. The study's findings align with the research conducted by Aziz and Andriansyah (2023), which highlights that self-learning systems ensure AI mechanisms stay updated as fraudulent tactics evolve, thereby maintaining their effectiveness. This adaptability also extends to phishing detection and IoT integration, offering a comprehensive defense against various fraudulent attempts.

Additionally, regulatory bodies conduct frequent audits and inspections to ensure compliance and also employees are well trained on compliance policies related to fraud prevention reveals that both statements had a minimum value of 1.00 and a maximum of 5.00. The mean was 3.72, (68.0%), implying that while employees feel **trained** on compliance, the percentage suggests that training programs might not be **comprehensive or frequent enough**, leaving room for further development. The standard deviation of 1.26 and 1.34 points to moderate dispersion, meaning some respondents may have experienced fewer audits than others. The research findings confirm the observations of Weske et al. (2018) about implementation actions requiring both appropriate actions and current levels of compliance motivation. The research indicates that one format of mandatory rule implementation does not provide superior results compared to other methods. Research conducted by Brown et al. (2024) showed that effective information security control proficiency leads employees to follow security policies thus stopping fraudulent activity in company computer systems.

Further regulatory penalties are a strong deterrent against fraudulent practices yielded a minimum value of 1.00 and a maximum value of 5.00, with a mean of 3.82 (70.5%) representing agreed. This indicates that most respondents believe regulatory penalties are a strong deterrent against fraudulent practices. A higher score suggests that employees generally believe regulatory penalties are effective deterrents, but there is still a moderate gap in full conviction of their deterrent power. The standard deviation of 1.19 is relatively lower than others, showing that responses were more clustered around the mean. This suggests a stronger consensus among bank employees that penalties from regulatory

bodies play an important role in discouraging fraudulent behavior. The research outcomes from Gonzalez and Hoffman (2018) parallel the study by showing that regular announcements of auditing results lack efficiency in preventing fraudulent activities. The effectiveness of such notifications depends on how well the monitoring system detects fraud.

The study nonetheless showed the highest level of agreement on the bank collaborates with regulators to enhance fraud detection and reporting, with a mean of 3.86 (71.5%). This higher score indicates a strong sense that the bank works effectively with regulators, which is seen as a positive aspect of fraud prevention. The minimum and maximum are remained at 1.00 and 5.00 respectively, while the standard deviation was 1.16, indicating less variability in responses compared to earlier items. This suggests that collaboration between banks and regulators is not only widespread but also consistently experienced across different institutions, enhancing overall fraud detection and reporting mechanisms. The research outcomes match the findings presented in Kamal, Alam, and Rahmani (2025), which demonstrated major implementation failures in internal controls together with four main bank fraud factors including insufficient employee training and excessive workload and competitive performance challenges and weak RBI guideline adherence.

The minimum and maximum scores for this statement were also 1.00 and 5.00, with a mean of 3.73 (68.3%) and a standard deviation of 1.30. These results imply that a majority of respondents agree that banks act on audit recommendations in a timely manner, although a portion of the respondents may have experienced delays or inconsistencies. The moderate standard deviation reflects some differences in how this practice is perceived or implemented across various institutions.

The study results showed that the bank promptly addresses audit recommendations from regulatory bodies, with responses ranging from 1.00 to 5.00. This variation indicates differing views among respondents. The mean score was 3.73, which translates to 68.25%, reflecting moderately strong agreement among participants. The standard deviation of 1.30 suggests a fair amount of variability in responses, meaning while many believe the bank responds well to audit feedback, others may see delays or inconsistencies in implementation. Research results match Cinaj et al. (2020) who explained auditors

maintain financial transparency and reliability while supervisors create systems confidence through their audits. Financial stability emerges through the auditors' ability to provide market participants with information that enables them to make intelligent decisions.

According to the findings, compliance officers actively monitor and enforce fraud prevention policies, with a minimum response of 1.00 and a maximum of 5.00. This range indicates a variety of perceptions. The mean score was 3.81, equal to 70.25%, indicating high agreement among respondents. Compliance officers are seen as effective, but there's still room for improvement in terms of enforcing policies to their fullest extent. The standard deviation of 1.26 shows some variability in responses, suggesting that although many employees recognize the role of compliance officers in enforcing policies, a few may feel the enforcement is not consistently applied. Research by Le, Vu and Nguyen (2021) supports these study findings because their studies revealed that internal control systems demonstrate negative significance towards law violations while not affecting public official bribe payments. Implementing codes of conduct decreases bribe payments to public officials yet does not impact law violations.

The percentage scores reflect a moderate-to-high level of agreement with the effectiveness of regulatory compliance efforts in the bank, with areas for improvement in training, policy enforcement, and addressing audit recommendations. The highest percentage score is seen in collaboration with regulators (71.5%), suggesting strong cooperation. Penalties and compliance monitoring also show a relatively high level of effectiveness. However, the lower scores for employee training (68.0%) and regulatory compliance (66.0%) suggest that more focused and frequent training, alongside better alignment with regulatory standards, could enhance fraud prevention efforts.

4.4.3 Descriptive Statistics Findings for Organizational Culture

The third objective of the study was to determine the effect of organizational culture on the occurrence of fraudulent activities in Kenyan commercial banks. The study results are presented in Table 4.12.

Table 4.12 Descriptive Statistics Findings for Organizational Culture

Statement	N	Minimum	Maximum	Mean	Stdv
1. Ethical behavior is encouraged and rewarded in our bank.	139	1.00	5.00	3.71	1.25
2. Management sets a good example in preventing fraudulent activities.	139	1.00	5.00	3.89	1.24
3. Employees are encouraged to report suspicious activities without fear of retaliation.	139	1.00	5.00	4.01	1.11
4. There are clear consequences for employees involved in fraudulent practices.	139	1.00	5.00	3.68	1.30
5. The bank promotes transparency and accountability in financial transactions.	139	1.00	5.00	3.68	1.32
6. The bank has a zero-tolerance policy for fraudulent activities.	139	1.00	5.00	3.77	1.32
7. Employees regularly receive ethics training to reinforce an integrity-driven culture.	139	1.00	5.00	3.76	1.29

$$\text{Percentage score for mean} = \frac{\text{Mean} - \text{Minimum}}{\text{Maximum} - \text{Minimum}} * 100$$

Studies presented in Table 4.12 confirmed that the bank rewards ethical behavior since respondents rated the practice between 1.00 and 5.00 points. The results indicate diverse perspectives because respondents showed approval and disagreement at various intensities. The participants indicated moderate agreement through their mean score of 3.71 that corresponded to 67.75% approval. Employees perceive that ethical behavior is somewhat rewarded, but there's a moderate level of agreement. Further encouragement could help build a stronger ethical culture. Variations exist within the responses regarding ethical conduct recognition and promotion in the bank since the standard deviation measure reached 1.25. The results of this investigation support Aman-Ullah and

Mehmood (2023) who discovered banking operations demand energetic staff who actively participate in work tasks. The implementation of IWEs (Innovative Work Environments) strengthens employee satisfaction as well as commitment and loyalty across the organization to produce enhanced long-term performance benefits.

Additionally, study findings demonstrates that management exemplifies high standards when it comes to preventing fraudulent activities by utilizing scores between 1.00 to 5.00. Multiple interpretations exist among the bank's employees about the topic. A majority of participants agreed to the extent that the mean score reached 3.89 which translates to 72.25% agreement. Management is seen as a positive example in preventing fraud, though the score indicates there could still be more leadership or proactive involvement in promoting fraud prevention. The 1.24 standard deviation indicates moderate dispersion because many staff members acknowledged management's fraud prevention leadership yet some staff members retained doubts about it. Maulidi and Ansell (2021) confirmed in their research that numerous fraud prevention techniques have emerged yet public sector organizations face difficulties in executing effective detection and prevention methods for fraud. The issue occurs from shortened fraud concepts matching with other organizational structures which enable fraud alongside unrecognized organizational dynamics that allow misconduct.

All employees engage in reporting suspicious activities since the bank provides protection against workplace retaliation as per investigation results. The study established minimum values of 1.00 and a maximum of 5.00. Various intensities exist within these reported opinions. The statement received the most agreement as employees scored 4.01 points which equated to 75.25% of the scale. The high score here suggests that employees are confident in reporting suspicious activities without fear of retaliation, indicating a strong culture of openness and whistleblower protection. This made it the highest agreement score across all statements. Customers' responses exhibit little variability through a standard deviation of 1.11 because they recognize the bank maintains a secure environment for whistleblowing.

Table 4.12 demonstrates employee sanction policies for fraudulent conduct based on responses from 1.00 to 5.00. The data indicates that respondents hold different opinions

on the subject. The measurement score reached 3.68 which demonstrated both moderate levels of agreement and 67.0% between participants. Employees feel there are consequences for engaging in fraud, but the moderate score indicates that the perception of enforcement may not be as strong as it could be. The measured standard deviation of 1.30 along with the studied responses indicates a reasonable amount of ambiguity on whether consequences exist or not. The research by Nawawi and Salin (2018) found that the company has adequate policies and standard operating procedures in place to address internal fraud and wrongdoing.

Financial transaction transparency and accountability at the bank received scores that spanned between 1.00 and 5.00 according to Table 4.12. The high score range points to conflicting opinions between study participants. The results show respondents agreeing to a moderate extent as the mean score reached 3.68 or 67.0%. There's a moderate level of agreement that transparency and accountability are promoted, suggesting that improvements can be made in these areas to ensure greater openness. Some employees maintain different perspectives about consistency in transparency and accountability practices because the measurement standard deviated from the mean by 1.32.

Findings also shows employees' responses regarding fraudulent activities policies at the bank stretched from 1.00 to 5.00. Responses vary significantly among the participants based on this measurement scale. The collected data measured at 3.77 which represents 69.25% of participants showing moderate agreement. The zero-tolerance policy is strongly endorsed, though the moderate score suggests some employees may not perceive it as consistently applied or adequately enforced. The banks clear position against fraud becomes less clear to some employees because their responses produce a standard deviation of 1.32. The research conducted by Barker (2018) about fraud prevention measures and e-security systems and co-liability consequences backs up the study's findings. The research developed prevention methods against possible harm to financial institutions and customers by introducing a proactive communication system that supports e-banking fraud prevention and co-liability framework.

Results in Table 4.12 demonstrate that regular ethics training is given to employees for maintaining an integrity-focused culture according to responses between 1.00 and 5.00.

Multiple viewpoints regarding this issue exist between respondents. Research data revealed that staff members had moderately strong agreement at 69.0% according to the mean score of 3.76. Regular ethics training is seen as an important part of reinforcing the culture, but the score implies there may be variability in how effectively the training is applied or engaged with by all employees. The net deviation of 1.29 between employee views demonstrates some diversity regarding their awareness of ethical training programs despite its established presence in the bank. Hidayah et al. (2024) reported results that matched the findings of this study showing governance and culture had minimal short-term influence on staff performance yet integrity and leadership significantly affected performance. Leadership emerged as a fundamental element that explains how integrity relates to organizational performance based on the research findings. Thus ethical and transparent practices gain great importance.

The percentage scores indicate that while the organizational culture in the bank is largely positive in terms of encouraging ethical behavior, preventing fraud, and promoting transparency, there are areas for improvement. The highest score was for the encouragement of whistleblowing (75.25%), suggesting a strong belief in reporting fraudulent activities without fear. However, areas such as consequences for fraud, training effectiveness, and promoting transparency could benefit from further attention and enhancement. The moderate scores on ethical behavior, consequences, and training indicate that these areas, while acknowledged, may not be perceived as fully effective by employees.

4.4.4 Descriptive Statistics Findings for Technological Advancement

The fourth objective of the study was to evaluate the effect of technological advancements on the occurrence of fraud in Kenyan commercial banks. The study results are presented in Table 4.13.

Table 4.13 Descriptive Statistics Findings for Technological Advancement

Statement	N	Minimum	Maximum	Mean	Stdv
-----------	---	---------	---------	------	------

1. The bank uses advanced fraud detection technology to monitor transactions in real-time.	139	1.00	5.00	3.82	1.25
2. Cybersecurity measures are regularly updated to prevent fraud.	139	1.00	5.00	3.88	1.15
3. Artificial intelligence and data analytics are used to detect fraudulent activities.	139	1.00	5.00	3.81	1.13
4. The online banking platform is secure against fraudulent activities.	139	1.00	5.00	3.85	1.17
5. Technology adoption has significantly reduced fraud in our bank.	139	1.00	5.00	3.78	1.25
6. The bank invests in continuous innovation to enhance fraud detection systems.	139	1.00	5.00	3.68	1.17
7. Employees are trained on emerging fraud-related cybersecurity threats.	139	1.00	5.00	3.62	1.23

$$\text{Percentage score for mean} = \frac{\text{Mean} - \text{Minimum}}{\text{Maximum} - \text{Minimum}} * 100$$

Table 4.13 demonstrates that the bank operates advanced fraud detection technology to track real-time transactions while respondents agreed minimally and maximally at 1.00 and 5.00 respectively. The wide distribution in responses covered total disagreement through full agreement with the statement. Participants showed a relatively high level of agreement as the obtained mean score equated to 70.5% (3.82). The moderate-to-high score indicates that employees perceive real-time fraud detection technology as relatively effective, though there may still be room for improvement in its implementation. The standard deviation at 1.25 indicates some variations because the participants did not have identical interpretations of present-time fraud detection technology effectiveness. The research by Kokogho et al. (2025) demonstrated that reshaped real-time auditing enabled

by blockchain technology creates both efficient operations combined with a sound and dependable financial system.

Findings also reveals that cybersecurity measure updates for fraud prevention take place on a regular basis as respondents chose rating values from 1.00 to 5.00. Different opinions prevail among the respondents regarding the matter at hand. Majority of the respondent agreed that cybersecurity measure updates for fraud prevention take place on a regular basis with 72.0% who rated 3.88 demonstrated strong agreement. The slightly higher score suggests that employees believe the bank is actively updating its cybersecurity measures, though there may still be ongoing threats that need continuous monitoring. Additionally, the respondent also agreed that regular cybersecurity measure updates based on the standard deviation of 1.15 which shows moderate variance but showed differing views among a few participants. The results from this study echo the research conducted by Paul et al. (2023) by demonstrating the vital need for robust security cultures in organizations together with employee training on damage risks and accountable management practices for client data. Financial organizations benefit from threat awareness groups because they exchange threat information through platforms that enable alliances and public-private defensive measures for joint cyber protection.

Artificial intelligence together with data analytics helps identify fraudulent activities according to the study findings. The scoring range for this practice extended from 1.00 to 5.00. The wide distribution demonstrates different views on this topic. The collected data revealed respondents shared similar perspectives because 70.3% of them rated the statement at 3.81. The use of AI and data analytics for fraud detection is viewed positively, but the score indicates that the integration of AI tools may not be fully optimized yet in detecting all fraudulent activities. The degree of variation is lower due to the standard deviation of 1.13 which indicates most respondents understood the fraud detection capabilities of AI and data analytics. Studies indicated by Ikhsan et al. (2022) support using advanced technology such as data analytics and artificial intelligence by the Indonesian Financial and Development Supervisory Agency to optimize fraud detection.

The security status of online banking platforms was established through Table 4.13 which showed responses between 1.00 and 5.00. The scale incorporates different responses from

participants to different views. The study results indicate that 71.3% or 3.85 on the scale demonstrated agreement among survey participants. Online banking security is perceived to be robust, with a moderate-to-high score indicating that while the system is secure, continuous improvements could further bolster cybersecurity defenses. The platform security receives moderate variability according to the standard deviation of 1.17 because respondents share both trust in the platform's security features and uncertainty about them. The findings confirm previous work by Phiri et al. (2024) who discovered banks have insufficient online fraud experts throughout the financial sector. Lack of expertise among banks leads to poor performance of their fraud detection systems according to the research findings.

The adoption of technology produced substantial fraud reduction across the banking institution according to study data that contained scores between 1.00 and 5.00. Different response patterns exist regarding this statement. The findings showed that 69.5% of the participants aged 3.78 point on average while maintaining at least moderate to high agreement. The moderate score reflects that while technology adoption is believed to have had an impact on reducing fraud, there is room for further technological investment or optimization to strengthen fraud prevention measures. Some differences exist in employee perceptions about technology's fraud reduction capabilities because the standard deviation stands at 1.25. The research by Akinbowale et al. (2024) revealed that combining internal and external anti-fraud systems which include filtering software and firewalls and encryption and continuous auditing and discovery sampling and virus protection and financial ratios and digital analysis and data mining can successfully prevent cyber fraud cases.

Results also shows a continuous investment of bank resources toward fraud detection system improvement through the responses given between 1.00 and 5.00. Diverse responses indicate employees do not share the same viewpoints regarding the topic. The survey results revealed moderate agreement since the respondents scored an average of 3.68 which corresponds to 67.0%. **Moderate investment** in innovation for **fraud detection systems** is perceived, suggesting that while the bank does invest in **innovation**, this investment may need to be **more continuous** or focused on specific fraud-related

technologies. The standard deviation at 1.17 indicates varied perceptions about the bank's innovative investments since several respondents doubt whether the bank provides enough or consistent support. The research findings match results from Adeyemo and Obafemi (2024) that showed participants reaching consensus about the beneficial influence of these technologies for detecting fraud early and promoting security.

The study showed that staff members undergo training regarding contemporary cyber threats relating to fraud which ranged from 1.00 to 5.00 points. The respondents display different degrees of alignment. The general assessment of 3.62 points revealed that employees showed moderate agreement at a rate of 65.5% for this subject yet this stood as the lowest among the entire category. The lowest score suggests that training programs related to cybersecurity threats are somewhat insufficient and could be enhanced to ensure employees are adequately prepared to deal with emerging fraud risks. The spread of results represented by a 1.23 standard deviation indicates reasonable variability because some workers either lacked training or remained unaware about it. Results from this study match Mwai et al.'s (2023) research that showed ICT risk assessment and ICT awareness had a weak non-significant link to information security implementation but information security audits created meaningful protection against insider fraud.

The percentage scores indicate a moderate-to-high level of agreement regarding the effectiveness of technological advancements in fraud detection and prevention. The highest score of 72.0% for cybersecurity measures suggests that the bank is perceived to be proactive in updating security systems. However, areas such as continuous innovation (67.0%) and employee training on cybersecurity threats (64.5%) suggest that more can be done to enhance the technological infrastructure and employee preparedness.

In summary, while technological advancements have had a positive impact on fraud reduction, further investment in innovation, training, and the integration of advanced tools like AI and data analytics is needed to address emerging threats and enhance the security framework of the bank.

4.4.5 Descriptive Statistics Findings for Fraudulent Practices

The study sought to assess the occurrence of fraud in Kenyan commercial banks. The results were presented as shown below. Findings are presented in Table 4.14.

Table 4.14 Descriptive Statistics Findings for Fraudulent Practices

Statement	N	Minimum	Maximum	Mean	Stdv
1. Have you ever witnessed or been aware of a fraud incident within the bank?	139	1.00	2.00	1.3741	.48564
2. How frequently do you believe fraud incidents occur in your department?	139	1.00	4.00	2.0719	.96038
3. In the past year, do you think fraud prevention measures (such as audits, checks, and balances) were effective in detecting fraud?	139	1.00	4.00	2.4245	1.07662
4. Do you think employees in your department are likely to report fraudulent behavior if observed?	139	1.00	3.00	2.1079	.86553
5. In your opinion, what is the biggest risk factor for fraud in the bank?	139	1.00	3.00	1.7554	.74056
6. Do you feel adequately trained to identify and report fraudulent activities?	139	1.00	2.00	1.3957	.49077
7. How often do you receive training on fraud prevention and reporting mechanisms?	139	1.00	4.00	2.3381	1.18904
8. Do you feel the bank's current fraud detection measures (e.g., monitoring systems, audits, etc.) are sufficient to prevent fraud?	139	1.00	3.00	2.0216	.86366

9. Have you observed any suspicious financial behavior in the past year that could indicate fraud?	139	1.00	3.00	1.8129	.82153
10. What actions do you believe should be taken to improve fraud prevention in the bank?	139	1.00	3.00	1.9712	.79803

$$\text{Percentage score for mean} = \frac{\text{Mean} - \text{Minimum}}{\text{Maximum} - \text{Minimum}} * 100$$

Table 4.14 revealed that staff members gave responses ranging from the minimum of 1.00 to the maximum of 2.00. These suggest that the respondent have ever witnessed or been aware of a fraud incident within the bank. The study results showed that the mean response was 1.37 (37%) the respondent agreed that they have ever witnessed or been aware of a fraud incident within the bank. This implies that Low awareness of fraud incidents, suggesting that employees rarely witness or are aware of fraud within the bank, which may indicate that fraud is not widespread or that reporting mechanisms need strengthening. The standard deviation of 0.49 indicates minimal variation in employee experiences on this matter. These findings are consistent with the research by Cholisoh and Hadziq (2021), which showed that, in part, the independent variables in Good Corporate Governance (GCG), such as information disclosure, accountability, responsibility, independence, and fairness, were found to have no impact on fraud financing.

Additionally, from a minimum of 1.00 to a maximum of 4.00, showing differing perceptions about how often fraud happens in their departments. The average mean was 2.07 (35.73%) which implies that fraud is considered to occur occasionally in various departments. Employees perceive that fraud incidents occur moderately in their department, which indicates a perception of risk but also suggests that not all employees perceive it as a frequent issue. A standard deviation of 0.96 shows noticeable variation in responses, meaning some departments may experience or suspect fraud more frequently than others. The results match Kagias et al. (2022) whose study showed private and public sector organizations face decreased funds alongside intensifying pressures that lead to

fraudulent activities. According to Dorris as President and CEO of the ACFE the upcoming years may witness an anticipated rise in fraudulent activities while he remembers the 2008 economic crisis situation when companies eliminated their non-profit generating departments including internal audit and compliance thus becoming more susceptible to fraud.

Respondents assessed fraud frequency across departments by using the minimum and maximum of 1.00 to 4.00 respectively. The staff assessment of fraud prevention systems yielded a 47.5% agreement level with a mean of 2.42 (47.5%). A moderate percentage score indicates that fraud prevention measures (audits, checks, and balances) are considered somewhat effective but with room for improvement. The standard deviation of 1.08 indicates both system trust from some employees and their lack of confidence in the systems among others. The research results by Moirangthem et al. (2022) shows that social conformism exists separately from system confidence as determinants of vaccine acceptance among healthcare and welfare professionals and both factors need consideration in vaccine promotional strategies.

The survey participants gave responses that were between a minimum value of 1.00 to a maximum value of 3.00 as the highest possible. The observed fraud reporting likelihood amounts to 55.4% when analyzed through the average score of 2.11. Moderate likelihood suggests that employees believe fraud is reported, but greater encouragement or safeguards may be needed to ensure higher reporting rates. The departments exhibit different levels of readiness to raise whistleblowing concerns according to the 0.87 standard deviation measurement. The results from this study match the research conducted by Choi and Gipper (2024) showing employees of fraudulent firms face reduced cumulative wages by 50% while showing elevated worker losses after fraud Caught Periods. The employment growth in fraud firms stays positive throughout fraud periods because these firms create extra staff positions and hire new employees who earn lower salaries although distressed firms mostly experience employee reductions.

The recorded responses for this question extended from a minimum of 1.00 to a maximum of 3. Employee perception of risk in particular operational areas stands at 37.8% according to the mean of 1.76. A moderate perception of risk factors suggests that employees see

vulnerabilities in the bank's systems but may not fully identify the most critical areas requiring attention. The standard deviation of 0.74 shows a fair level of consistency in responses across staff. The results from this research match Hadian et al. (2021) when they evaluated internal control and fraud detection at state-owned banks in Bandung to be at a good level. Internal control plays a substantial role in detecting fraud according to research findings since the effect stems from internal control (56%) and outside factors (44%) that influence the variable.

The participant responses for this question spanned from 1.00 to 2.00. Survey results show that 39.6% of employees do not possess enough training to detect fraud according to the mean score of 1.40. The low score indicates that employees feel insufficiently trained to identify and report fraudulent activities, pointing to a training gap in fraud prevention. Data show that staff members have similar opinions regarding the requirement for enhanced training because standard deviation stands at 0.49. The research results by DeZoort and Harrison (2018) demonstrated that professional obligation combined with personal control creates significant effects on responsibility but fail to show any relationship with task clarity. The study revealed that perceived responsibility enhances the quantity of detection procedures people brainstorm and it functions as a factor that weakly links accountability to detection brainstorming.

The survey collected responses that varied from 1.00 through to 4.00. The average rating at 2.34 represents a 44.6% agreement which demonstrates that staff members receive occasional fraud prevention training instead of regular sessions. Employees report receiving moderate levels of training. This suggests that the frequency or depth of training needs to be enhanced to ensure better preparedness for fraud detection. High variability between departments or roles emerges from the wide distribution of responses indicated by a standard deviation value of 1.19. This implies that while a portion of the respondents regularly receive training on fraud prevention and reporting mechanisms, a significant number either receive it infrequently or not at all, indicating inconsistency in training efforts and the need for more comprehensive and regular capacity-building programs to enhance fraud awareness and reporting across the organization (Hashim et al., 2020).

Additionally, the study findings also indicates that responses ranged from 1.00 at the minimum and to 3.00 at the maximum. The bank received a moderate 51.08% confidence rating in their fraud detection performance as shown by the mean score of 2.02(51.08%) agreement. The moderate score implies mixed perceptions of fraud detection systems, suggesting that while some employees feel satisfied, others may think more robust measures are necessary. The standard deviation measures 0.86 indicating departments are uniformly spread in their trust levels yet there are pockets of departments that put more faith in the systems than others do.

The study findings further indicates that the maximum of 1.00 and minimum of 3.00 if they have ever observed any suspicious financial behavior in the past year that could indicate fraud. Moderate awareness of suspicious activities indicates that employees may have noticed potential fraud, but either it was not reported or not recognized as fraud. A significant number of staff members agreed to have seen or observed any suspicious financial behavior in the past year that could indicate fraud of 1.8129. A standard deviation of 0.82 signifies the existence of suspicious financial behavior in the past year that could indicate fraud. These findings are consistent with the research by DeLiema et al. (2020), which found that only a few HRS respondents mentioned any specific form of fraud over the past 5 years. However, 5.0% reported experiencing at least one form of investment fraud, while 4.4% recounted prize or lottery fraud.

Finally, the study findings indicates that the minimum value of 1.00 and a maximum of 3.00 was used to survey what actions should be taken to improve fraud prevention in the bank. The study findings indicates that actions should be taken to improve fraud prevention in the bank with mean of 1.97(48.56%). Moderate agreement suggests that employees believe there is room for improvement in fraud prevention, but the suggestions for improvement might need further clarification or prioritization. This 0.80 standard deviation shows standard agreement between departments even though certain departments possess stronger views about required improvements. The study's findings align with the research by Hardika and Lubis (2021), which found that both the whistleblowing system and internal control play a significant role in fraud prevention.

This study offers valuable insights for unit leaders to enhance whistleblowing system facilities and internal controls, based on input and experiences related to individual performance in improving fraud prevention.

The percentage scores provide insight into how employees perceive fraudulent practices within the bank. The findings suggest a moderate level of awareness of fraud incidents and a moderate confidence in fraud prevention measures. However, there are several areas for improvement, particularly in terms of employee training, reporting mechanisms, and enhancing fraud detection systems. The lowest score for adequate training to identify and report fraud (39.89%) points to a key area for intervention, where more comprehensive and frequent training could significantly improve fraud detection and prevention within the bank.

4.4.6 Descriptive statistics Findings for staff training

The study sought to assess the staff trading (moderator). The results were presented as shown below. The study results are presented in Table 4.15.

Table 4.15 Descriptive statistics Findings for staff training

Statement	N	Minimum	Maximum	Mean	Stdv
1. Employees receive regular training on fraud prevention and detection.	139	1.00	5.00	3.76	1.29
2. The bank provides periodic workshops on regulatory compliance and ethics.	139	1.00	5.00	3.81	1.21
3. Staff members are trained to use fraud detection technology and tools.	139	1.00	5.00	3.76	1.17
4. Employees are well-equipped to recognize and report fraudulent activities.	139	1.00	5.00	3.84	1.19

5. Training programs enhance employees' ability to adhere to internal control policies.	139	1.00	5.00	3.76	1.27
6. Fraud prevention training is tailored to specific roles within the bank.	139	1.00	5.00	3.64	1.19
7. Employees receive refresher courses on fraud prevention and compliance policies.	139	1.00	5.00	3.65	1.26

$$\text{Percentage score for mean} = \frac{\text{Mean} - \text{Minimum}}{\text{Maximum} - \text{Minimum}} * 100$$

Table 4.15 revealed that staff members receive ongoing training on fraud prevention and detection which ranges throughout the scale from 1.00 to 5.00. Different employees displayed varying levels of approval and opposition about this topic. The survey data demonstrated that employees agree moderately strongly with the statement since their average response achieved a score of 3.76 which translates to 69.0 percent agreement. Staff members display varying opinions about their training consistency because the data shows standard deviation at 1.29. Moderate frequency of training indicates that while employees receive training on fraud prevention, there is potential for greater regularity or depth in these training programs. The study's findings are consistent with the research by Abu Amuna and Abu Mouamer (2020), which found that respondents gave a positive evaluation regarding the levels of application of tools to detect and prevent job fraud within the Ministry of Health (MOH). Additionally, the study highlighted a strong interest in using these tools to prevent job fraud during the implementation of various tasks.

The bank organizes periodic workshops on regulatory compliance and ethics which receive responses between 1.00 and 5.00 according to Table 4.24. This range indicates differing perceptions. A survey analysis showed that 70.25% of the respondents (or 3.81 on the scale) held similar views on this matter. Good provision of workshops on regulatory compliance and ethics suggests that the bank is proactive in this area, but there is still room for further workshops or updates on evolving regulations. The standard deviation rating of 1.21 shows moderate response variability since most employees have access to such workshops but some have experienced them less frequently or not at all.

The results established that staff members get training regarding fraud detection technology tools through multiple rating points between 1.00 and 5.00. The data displays different opinions within this range. Staff members displayed moderate agreement based on the mean score of 3.76 which equated to 69.0%. Training on fraud detection tools appears to be moderately effective, but more focus might be required on ensuring that employees are proficient in using the technology at their disposal. Many employees went through technical training according to the standard deviation of 1.17 yet some staff members did not feel sufficiently prepared. The study's findings align with the research by Hassan et al. (2025), which indicates that strong corporate governance (CG) practices and IT techniques are crucial in detecting and reducing fraudulent activities by minimizing opportunities, rationalizations, pressures, and the capabilities of potential employees to commit fraud. Additionally, internal controls play a significant role in decreasing instances of fraud.

Table 4.24 showed that employees demonstrate good abilities to detect and report fraud through their responses between 1.00 and 5.00. Several respondents take different approaches regarding this issue. The questionnaire showed that 71.0% of staff members agree employees can both spot and report fraudulent activities through their responses with an average of 3.84 points. The higher score indicates that employees feel relatively well-equipped to handle fraud detection, suggesting good training practices, though there may still be gaps in specific areas of fraud reporting. The data shows a moderate level of variability since the 1.19 standard deviation indicates different readiness levels exist based on roles and training requirements. Research conducted by Baten, (2020) found that one of the most effective strategies to discourage dishonest behavior is to inform employees of the company's policy. Preventing fraud requires adhering to the policy and implementing the specified actions and penalties when someone is discovered.

Survey participants rated training programs as effective for employee internal control policy adherence by distributing their responses between 1.00 and 5.00. A broad range of stands exists throughout the survey results. Most agree that internal control readiness stands at 69.0% as shown through the mean score of 3.76. Moderate effectiveness in adherence to internal controls suggests that training on these policies exists but could be

made more targeted to improve compliance among employees. Some variability exists between employees who believe training works effectively while others think it requires enhancement according to the standard deviation of 1.27. The study's findings are consistent with the research by Oyelakin and Abdullahi (2022), which showed that employee training, control environment, information and communication, and risk assessment have a significant and positive impact on the financial management of SMEs. Control activities were found to have a positive but insignificant effect, while monitoring activities had a negative and significant effect on the financial management of SMEs.

Fraud prevention training matches roles at the bank and generates scores between 1.00 and 5.00 according to Table 4.24. The measured data displayed in this range reveals that members of the sample had different perceptions about the level of role-specific training received. The calculated mean value equaled 3.64 which indicated 66.0% agreement and reflective of moderate concurrence. The moderate score reflects that role-specific training is inadequate, which could hinder employees' ability to respond to fraud risks that are unique to their specific roles. The 1.19 standard deviation indicates response fluctuation indicating that the implementation or experience of role-based training differs between departments. The study's findings align with the research by Trehan (2024), which highlights the significant role of forensic accounting training in strengthening the banking sector's resilience against fraudulent practices. The study also emphasizes the implications of this training for regulatory compliance, risk management, and organizational governance.

The research data indicated that employees participate in periodic fraud prevention training sessions which are assessed between 1.00 and 5.00 on the scale. Multiple opinions exist among survey participants according to this finding. The 3.65 rating equates to moderate agreement at the 66.25% level. The moderate score indicates that refresher courses on fraud prevention are offered, but they could be more frequent, relevant, or specific to emerging fraud tactics. The noticed variation in employee perceptions of regular refresher training emerges from a standard deviation measurement of 1.26. Research conducted by Hina and Dominic, (2020) indicates that the awareness of security

dangers and the communication of information security rules to end users (workers) are still lacking in HEIs, as is ISPC.

The percentage scores reveal that fraud prevention and detection training within the bank is perceived as moderately effective. The highest score is for equipping employees to recognize and report fraudulent activities (71.0%), indicating that employees generally feel confident in their ability to detect and report fraud. However, there are areas for improvement, especially in providing role-specific training (64.0%) and refresher courses (64.5%). While the bank provides valuable training programs, there are areas where the training can be enhanced to ensure that all employees, across different roles, are fully prepared to detect and prevent fraud effectively. More frequent and tailored training, along with refresher courses, could strengthen the bank's fraud prevention efforts and ensure that employees are always equipped with the latest knowledge and skills to combat fraud.

4.5 Inferential Statistics

In this section, the study tested linearity, homoscedasticity, normality and multicollinearity tests.

4.5.1 Linearity Test

A linearity test was conducted to determine whether the relationship between the dependent and independent variables is linear or non-linear. According to Gujarati and Porter (2011), when the relationship is linear, multiple linear regression can be appropriately applied. A non-linear relationship underestimates the coefficient of the regression results. The linearity of the data indicates that for each incremental change in an independent variable, the dependent variable's values follow a straight-line pattern. The results of the linearity analysis are presented in Table 4.16.

Table 4.16 Test of Linearity

Variables	Linearity	Deviation from Linearity
Internal control system	.000	.203
Regulatory compliance	.000	.622
Organizational culture	.000	.110
Technological advancement	.000	.334

Staff training	.000	.171
----------------	------	------

Table 4.16 contains data about the deviation from linearity and linearity values for the internal control system, which were 0.203 (greater than 0.05) and 0.000 (less than 0.05), respectively. For regulatory compliance, the deviation from linearity and linearity values were 0.622 (greater than 0.05) and 0.000 (less than 0.05), respectively. The findings also revealed that organizational culture had deviation from linearity and linearity values of 0.110 (greater than 0.05) and 0.000 (less than 0.05), respectively. Similarly, technological advancement showed deviation from linearity and linearity values of 0.334 (greater than 0.05) and 0.000 (less than 0.05), respectively. Finally, staff training had deviation from linearity and linearity values of 0.171 (greater than 0.05) and 0.000 (less than 0.05), respectively. The linearity values evaluated for the four variables and the moderator lay below 0.005 which supports the assumption of linearity. The data analysis for each of the five study variables found deviation from linearity values exceeding 0.05 because none of these variables deviated from linearity.

4.5.2 Homoscedasticity Test

Homoscedasticity test checks whether there is equal spread or equal variance in the residual variance of the period under observation (Gujarati & Porter, 2011). The homoscedasticity assumption was assessed using Levene's test for equality of error variances. The results of the assumed-true-positive tests are presented in Table 4.17.

Table 4.17 Homoscedasticity Assumption

Variable	Levene Statistic	df1	df2	Sig.
Internal control system	19.701	2	136	.106
Regulatory compliance	37.086	2	136	.140
Organizational culture	0.888	2	136	.414
Technological advancement	7.380	3	135	.129
Staff training	13.101	2	136	.126

The results presented in Table 4.17 show that the p-values from Levene's test for the various variables were as follows: 19.701 for the internal control system, 37.086 for regulatory compliance, 0.888 for organizational culture, 7.380 for technological advancement, and 13.101 for staff training. The data passed the homoscedasticity assumption because all p-values exceeded 0.05. This result means the data did not show heteroscedasticity patterns.

4.4.3 Normality Test

The research used Shapiro-Wilk statistics to determine if the data showed substantial differences compared to normal distribution. The data deviates from normality when the significance value becomes smaller than 0.05 according to Ghasemi and Zahediasl (2012). Table 4.18 presents the findings obtained from the test execution.

Table 4.18 Normality Assumption Test

	Shapiro-Wilk		Sig.
	Statistic	df	
Internal control system	.543	22	.140
Regulatory compliance	.644	16	.123
Organizational culture	.476	101	.164
Technological advancement	.587	24	.147
Staff training	.788	18	.102

The Table 4.18 data shows that every Shapiro-Wilk value met statistical significance when passing the 0.05 threshold. Data conventionally follows normal distribution because all the significance levels were below 0.05. The Kolmogorov-Smirnov test indicates normal distribution when the obtained value stays under 0.05 (Ahad, Yin, Othman, & Yaacob, 2011).

4.4.4 Multicollinearity Test

The study checked for Multicollinearity through Variances Inflation Factor (VIF) measurements and tolerance factor tests. The extent of multicollinearity can be evaluated using a tolerance value between 1 and 0 (Curto & Pinto, 2007; Schieren & Carr, 1982). The VIF helps determine how much the coefficient estimate variance increases because of multicollinearity. One of the independent variables exhibited the maximum VIF for evaluation. The research data obtains evaluation through Table 4.19 for multicollinearity testing.

Table 4.19 Multicollinearity Test

Variables	Tolerance	VIF
Internal control system	.723	1.383
Regulatory compliance	.639	1.566
Organizational culture	.593	1.687
Technological advancement	.537	1.861
Staff training	.756	1.323

Table 4.19 demonstrates tolerance and Variance Inflation Factor (VIF) readings for internal control system at 0.723 with 1.383 while regulatory compliance stands at 0.639 with 1.566. Organizational culture maintains 0.593 and 1.687 and technological advancement has 0.537 and 1.861 followed by staff training at 0.756 and 1.323. Multicollinearity does not present major issues in the dataset based on the results of tolerance and VIF values. According to Hair, Ringle, and Sarstedt (2013), a VIF greater than 5 (or a tolerance value less than 0.20) would indicate poorly estimated regression coefficients due to multicollinearity, but this was not the case in this study.

4.5 Correlation Analysis

Correlation refers to the extent of the relationship between two variables. The variables show a strong connection if their correlation is high yet weak relations emerge from low

correlations. The Pearson Correlation stands as the dominant technique used for correlation measurement among researchers. The outcome table appears in Table 4.20.

Table 4.20 Correlation Analysis

		Y	X1	X2	X3	X4	M
Y	Pearson Correlation	1					
	Sig. (2-tailed)						
X1	Pearson Correlation	.550**	1				
	Sig. (2-tailed)	.000					
X2	Pearson Correlation	.561**	.459**	1			
	Sig. (2-tailed)	.000	.000				
X3	Pearson Correlation	.600**	.409**	.502**	1		
	Sig. (2-tailed)	.000	.000	.000			
X4	Pearson Correlation	.606**	.408**	.470**	.569**	1	
	Sig. (2-tailed)	.000	.000	.000	.000		
M	Pearson Correlation	.488**	.277**	.315**	.293**	.480**	1
	Sig. (2-tailed)	.000	.001	.000	.000	.000	
	N	139	139	139	139	139	139

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

Key: Y= fraudulent practices detection, X_1 = Internal Control, X_2 = Regulatory Compliance, X_3 = Organizational culture, X_4 = Technological Advancements and M = Moderator (staff training)

Results from Table 4.20 show a strong correlation with 0.550 significance that exists between fraud detection and internal control systems ($p < 0.01$). The quality enhancement of internal controls produces greater chances of catching deceptive practices. The analysis found regulatory compliance produced a substantial positive correlation of 0.561 with fraud detection ($p < 0.01$). Higher compliance levels within organizations lead to better abilities for fraud detection. Fraud detection shows a powerful connection to organizational culture based on the statistical correlation of $r=0.600$ ($p < 0.01$). Business organizations having good organizational structure demonstrate stronger abilities to detect fraudulent events.

Research evidence shows a significant positive relationship exists between fraud detection capabilities and technological development levels ($r= 0.606$; $p<0.01$). Modern organizations that implement advanced technological systems possess better fraud detection capabilities. The relationship between staff training and fraud detection showed a statistically significant moderate positive correlation value at $r=0.488$ ($p < 0.01$). Staff training plays a role in detecting fraud however its impact is less significant when compared to organizational culture and technological advancement.

4.6 Hierarchical Moderated Regression Analysis

Staff training served as the moderating variable for analyzing the relationship between the independent and dependent variables. The researchers used hierarchical linear regression analysis to investigate the moderation effects according to Baron and Kenny (1986). A regression analysis evaluated the single moderating influence of every variable between independent and dependent variables.

Table 4.21 Hierarchical Moderated Regression Analysis

Variables	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6
(Constant)	0.064(.741)	-0.177(.397)	0.016(.943)	-0.044(.880)	0.124(.563)	0.121(.564)
Internal control system	0.250(.000)	0.235(.000)	0.134(.107)	0-.101(.398)	-0.009(.942)	0.005(.965)
Regulatory compliance	0.185(.007)	0.166(.013)	0.164(.013)	0.481(.001)	0.800(.000)	0.847(0.000)
Organizational culture	0.257(.001)	0.252(.001)	0.252(.001)	0.217(.004)	-0.202(.155)	-0.069(0.635)
Technological advancement	0.279(.000)	0.192(.014)	0.213(.006)	0.240(.002)	0.240(.001)	-0.015(0.888)
Staff training		0.209(0.002)	0.102(0.226)	0.160(0.062)	0.051(0.561)	0.057(0.505)
Staff training × Internal control system			0.050(0.047)	0.137(0.001)	0.091(0.028)	0.083(0.042)
Staff training × Regulatory compliance				-0.126(0.009)	-0.240(0.000)	-0.262(0.000)
Staff training × Organizational culture					0.181(.001)	.125(0.024)
Staff training × Technological advancement						0.096(0.006)
F statistic	42.453	38.353	33.350	30.930	30.805	29.640
R ²	0.559	0.590	0.603	0.623	0.655	0.674
R ² change	0.559	0.032	0.012	0.021	0.032	0.019

Table 4.21 reports a coefficient of determination (R²) of 0.559. The results indicate a significant statistical relationship at $p < 0.05$ between independent variables which jointly

explain 55.9% of employee fraud occurrence in Kenyan commercial banks. The 0.505 value determines how well the independent variables explain the research. These variables included the internal control system, regulatory compliance, organizational culture, and technological advancement.

Additionally, Table 4.21 presents the results of the R^2 changes. From model 1 to model 2, the R^2 increased by 0.032, from 0.559 to 0.590, and this change was statistically significant ($p < 0.05$). This suggests that the inclusion of staff training in the model enhanced its predictive ability in forecasting the occurrence of fraudulent practices by increasing the explained variance by 3.2%.

From model 2 to model 3, the R^2 increased by 0.012, from 0.590 to 0.603, which was also statistically significant ($p < 0.05$). This change indicates that staff training moderates the effect of the internal control system on the occurrence of fraudulent practices, contributing an additional 1.2% of explained variance.

From model 3 to model 4, the R^2 increased by 0.021, from 0.603 to 0.623, and this change was statistically significant ($p < 0.05$). This suggests that staff training moderates the effects of both the internal control system and regulatory compliance on fraudulent practices, contributing an additional 2.1% to the explained variance.

From model 4 to model 5, the R^2 increased by 0.032, from 0.623 to 0.655, and this change was statistically significant ($p < 0.05$). This demonstrates that staff training enhances the effects of the internal control system, regulatory compliance, and organizational culture on fraudulent practices, contributing an additional 3.2% of explained variance.

Based on the transition from model 5 to model 6 the R^2 value rose by 0.019, progressing from 0.655 to 0.674 and this statistical change reached significance ($p < 0.05$). The implementation of staff training sessions serves as a moderator to enhance the explanatory power of internal control systems along with regulatory compliance and organizational culture and technological advancement in preventing fraudulent practices by 1.9%.

Table 4.21 contains F-test information which defines the validity of the regression models created. The F-statistic value for model 1 reached 42.453 while its corresponding R-

squared value equaled 0.559 establishing the significance of independent variables in explaining dependent variables ($F = 42.453, p < 0.05$). The appropriateness of the model fit exists because internal control together with regulatory compliance and organizational culture and technological training affect fraudulent activity levels in Kenyan commercial banks.

Model 2 produced an F-value of 38.353 along with an R^2 of 0.590 that resulted in an R^2 change of 0.032. Staff training participation within the model enhanced both the model fit and fraudulent practices prediction performance ($F = 38.535, p < 0.05$).

Model 3 predicted 0.603 of the total variance through its F-value of 33.350 combined with an R^2 change of 0.012 which demonstrates that staff training moderating the internal control system enhanced model prediction power ($F = 33.350, p < 0.05$).

A better explanatory power emerged when examining staff training effects on internal control system and regulatory compliance through model 4 which yielded an F-value of 30.930 alongside an R^2 of 0.623 and an R^2 change of 0.021 ($F = 30.930, p < 0.05$).

The value of F for model 5 amounted to 30.805 while its R^2 reached 0.655 with an R^2 change of 0.032. Staff training resulted in better discriminatory power for detecting fraudulent activities when it acted as a moderator between internal controls and regulatory compliance and organizational cultural elements ($F = 30.805, p < 0.05$).

Model 6 reached an F-value of 29.640 as its R^2 measurement resulted in 0.674 and an R^2 change value of 0.019. The model fits better after staff training implementation because it moderates the effect of internal control alongside regulatory compliance and organizational culture while benefiting from technological progressions ($F = 29.640, p < 0.05$).

The regression coefficients in model 1, as presented in Table 4.22, indicate that each independent variable had a significant positive effect on the occurrence of fraudulent practices. Specifically, the internal control system ($\beta_1 = 0.250, p < 0.05$), regulatory compliance ($\beta_2 = 0.185, p < 0.05$), organizational culture ($\beta_3 = 0.257, p < 0.05$), and

technological advancement ($\beta_4 = 0.279, p < 0.05$) all contributed significantly to the occurrence of fraudulent practices among employees in Kenyan commercial banks.

In model 2, the regression analysis showed that staff training significantly influenced the relationship between the independent variables and fraudulent practices, with a coefficient of staff training interaction being 0.000, which is less than 0.05. This suggests that staff training plays a role in moderating the relationship between the independent variables and fraudulent practices.

In model 3, staff training was found to have a significant moderating effect on the relationship between the internal control system and fraudulent practices ($\beta = 0.050, p < 0.05$). The coefficient of staff training interaction had a p-value of 0.047, confirming its significance in moderating this relationship.

The relationship between internal control system and fraudulent practices received a significant positive impact from staff training whereas regulatory compliance relations to fraudulent practices received a negative impact ($\beta = 0.137, p < 0.05$) and ($\beta = -0.126, p < 0.05$), respectively.

Lack of training among staff members strengthened both the relationship between internal control systems and fraudulent practices ($\beta = 0.091, p < 0.05$) and organizational culture and fraudulent practices ($\beta = 0.181, p < 0.05$) yet weakened the relationship between regulatory compliance and fraudulent practices ($\beta = -0.240, p < 0.05$).

Staff training created significant outcomes in model 6 by moderating the pathways where internal control system ($\beta = 0.083, p < 0.05$), organizational culture ($\beta = 0.125, p < 0.05$) and technological advancement ($\beta = 0.096, p < 0.05$) linked to fraudulent practices while exhibiting negative associations on the regulatory compliance to fraudulent practices relationship ($\beta = -0.262, p < 0.05$).

$$Y = 0.064 + 0.250X_1 + 0.185X_2 + 0.257X_3 + 0.279X_4 + 0.209Z + 0.083Z * X_1 - 0.262Z * X_2 + 0.125Z * X_3 + 0.096Z * X_4$$

4.7 Chapter summary

This chapter has outlined the results findings and discussions. The study achieved a high response rate of 91.4%, with 139 completed questionnaires returned from the 152 distributed. This indicates a robust participation rate, with only 8.6% of respondents failing to return the questionnaires. Cronbach's alpha values ranged from 0.710 to 0.826, indicating a strong level of reliability across the different variables such as internal control systems, regulatory compliance, organizational culture, technological advancement, and staff training. The demographic analysis of the respondents revealed that the gender distribution was relatively balanced, with 51.8% of respondents being male and 48.2% female. Age-wise, the majority of respondents (38.8%) were between 26 and 35 years old. In terms of education, 38.1% held a bachelor's degree. Regarding job positions, 37.4% worked as risk managers.

These findings suggest that internal controls, though effective, still have areas that may need improvement or greater clarity among employees. Regulatory compliance measures, including regular audits, employee training, and regulatory penalties. Respondents generally agreed that the banks complied with regulatory requirements, and penalties were an effective means of discouraging fraudulent activities.

The study found that organizational culture plays a pivotal role in fraud prevention. Technological advancements, including real-time fraud detection systems, regular cybersecurity updates, and the use of artificial intelligence for fraud detection, were viewed positively by the respondents. Staff training emerged as a critical factor in enhancing employees' ability to detect and prevent fraud.

Linearity, Homoscedasticity and Normality Tests confirmed that the data met the assumptions required for regression analysis, as the linearity, homoscedasticity, and normality tests did not reveal any significant issues. Correlation Analysis: The correlation analysis indicated that fraud detection was strongly correlated with factors like internal control ($r=0.550$), regulatory compliance ($r=0.561$), organizational culture ($r=0.600$) and technological advancements ($r=0.606$). Staff training showed a moderate positive correlation ($r=0.488$) with fraud detection. Hierarchical Moderated Regression Analysis found that staff training was found to significantly moderate the relationship between the

factors influencing fraudulent practices and fraud detection. The analysis showed that staff training enhanced the effectiveness of internal controls, regulatory compliance, organizational culture and technological advancements in preventing fraud.



CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The findings together with conclusions and suggested solutions form the basis of this section for this report. Future research possibilities are presented in the following subsections.

5.2 Summary of the Study Findings.

The research objectives receive a summary of study findings in this segment.

5.2.1 Effect of internal control systems

This research investigated how internal control systems influence fraudulent employee conduct in Kenyan commercial banking institutions. The research showed that most survey participants accepted bank has a whistleblowing mechanism that helps in reporting fraudulent activities and also, they agreed that the bank has effective internal control systems that prevent fraudulent activities.

Additionally, the respondent agreed that regular risk assessments are conducted to identify fraud risks and also, they agreed that there are clear policies and procedures in place to mitigate fraud. Furthermore, employee roles and responsibilities are well defined to prevent unauthorized transactions, they also agreed that the internal audit department effectively monitors fraud risks and irregularities and finally they agreed that internal control measures are regularly reviewed and updated to address emerging fraud risks.

5.2.2 Effect of regulatory compliance

The research examined how regulatory compliance affects the occurrence of fraud within Kenyan commercial banks as its secondary goal. Most respondents confirmed through study results that the bank adheres to every fraud prevention regulatory requirement along with consistent audits from regulatory bodies for compliance verification.

Most respondents confirmed their agreement with the statement about proper training of employees to follow fraud prevention policies and with the effectiveness of regulatory penalties to prevent fraudulent conduct. Further, the study findings reveal that the bank

collaborates with regulators to enhance fraud detection and reporting and also, they agreed that the bank promptly addresses audit recommendations from regulatory bodies and finally they agreed that compliance officers actively monitor and enforce fraud prevention policies.

5.2.3 Effect of organizational culture

The objective of this research examined how organizational culture affects fraudulent activities within Kenyan commercial banks. Results from the study showed that our bank encourages ethical conduct and awards people who follow ethical standards and that management demonstrates exemplary behavior to prevent fraudulent activities. In addition to these agreements the respondents also stated that employees can safely report suspicious matters without facing retaliation from the bank and they confirmed the presence of strict penalties for employees participating in fraudulent conduct.

The research shows that the participant endorses bank transparency and financial accountability standards as well as supporting the bank's strict policy against major fraud and the widespread training programs for workforce ethical development.

5.2.4 Effect of technological advancements

The analysis determined how technological advancements influence fraud occurrence within Kenyan commercial banks. The study results indicate that the respondent agreed that the bank uses advanced frauds detection technology to monitor transactions in real-time and also, they agreed that cybersecurity measures are regularly updated to prevent fraud.

Majority of the respondent agreed that artificial intelligence and data analytics are used to detect fraudulent activities and also, they agreed that the online banking platform is secure against fraudulent activities. The study further reveals that and also they agreed that technology adoption has significantly reduced fraud in our bank. Findings also indicate that the bank invests in continuous innovation to enhance fraud detection systems and finally they agreed that employees are trained on emerging fraud-related cybersecurity threats.

5.2.5 Staff training

This research investigated the staff training influence which affects the relationship between factors leading to fraudulent behavior within Kenyan commercial banking institutions. Most participants in the study confirmed that staff members access regular training about fraud prevention and detection methods and the bank delivers periodic workshops about regulatory compliance combined with ethics. Additionally, they agreed that staff members are trained to use fraud detection technology and tools. Majority of the respondent also agreed that employees are well-equipped to recognize and report fraudulent activities.

Further, they also agreed that training programs enhance employees' ability to adhere to internal control policies and also, they agreed that fraud prevention training is tailored to specific roles within the bank and finally they agreed that employees receive refresher courses on fraud prevention and compliance policies.

5.3 Discussion

This section contains discussion of the findings

5.3.1 Effect of internal control systems

This research aimed to examine how internal control systems influence fraudulent employee conduct in Kenyan commercial banks. The findings revealed that the majority of respondents believed the bank had effective internal control systems in place, including a whistleblowing mechanism, clear fraud prevention policies, regular risk assessments, and well-defined employee roles to prevent unauthorized transactions. Additionally, respondents agreed that internal audit departments effectively monitor fraud risks and that internal controls are regularly reviewed to address emerging fraud risks. The findings of this study agreed with Ilugbusi et al. (2020), who found that comprehensive risk assessments significantly reduce fraud in Nigerian banks. Similar to this study, Kenyan banks also emphasize the importance of risk management as a crucial aspect of internal control systems for fraud prevention. Both studies underscore the role of risk assessments in preventing fraudulent activities. This study also agrees with Chen and Elder (2021), who emphasized the importance of monitoring systems and risk assessments in U.S. banks for reducing fraud. Both studies highlight the essential role of regular monitoring and

evaluation of internal control systems to prevent fraud, showing consistency across different banking contexts. However, the technological infrastructure in Kenyan banks may not be as advanced as in U.S. banks, which can affect the implementation of such systems.

The findings in this study disagree with Ogola (2015), who highlighted that poor management oversight and lack of segregation of duties were critical weaknesses in Kenyan banks' internal control systems. Ogola's study pointed out that these weaknesses contributed significantly to fraud, whereas this study's findings indicated that respondents felt their banks had effective internal controls in place. This disagreement may be due to the institutional context, as Ogola's study focused on specific Kenyan banks, while this research surveyed a broader sample, possibly including banks with stronger oversight mechanisms. While both Adegbite et al. (2021) and Molefe and Mkhize (2023) argue that weak enforcement of internal controls increases fraud risks, this study's findings suggest that respondents felt internal controls in Kenyan banks were effectively enforced. This discrepancy may arise from differences in perceptions of enforcement, with this study finding that employees generally felt confident in the monitoring systems in place, while previous studies noted that lax enforcement of controls led to increased fraud.

The findings support Cressey's Fraud Triangle Theory (1953), particularly the 'opportunity' aspect of the triangle. According to Fraud Triangle Theory, when internal controls are weak, the opportunity for fraud increases. However, in this study, the presence of strong internal controls, such as whistleblowing mechanisms and well-defined roles, reduces this opportunity. This aligns with the idea that robust internal controls can significantly mitigate the chances of fraud occurring.

5.3.2 Effect of regulatory compliance

This research investigated how regulatory compliance affects the occurrence of fraud within Kenyan commercial banks. The study revealed that most respondents confirmed that their banks adhere to all fraud prevention regulatory requirements and consistently undergo audits from regulatory bodies to ensure compliance. Additionally, most respondents agreed that employees are well-trained to follow fraud prevention policies, and they affirmed the effectiveness of regulatory penalties in deterring fraud. Furthermore,

respondents confirmed that the bank collaborates with regulators to enhance fraud detection and reporting, and that the bank promptly addresses audit recommendations from regulatory bodies. Finally, respondents noted that compliance officers actively monitor and enforce fraud prevention policies. The findings in this study agree with Olojede et al. (2020), who found that regulatory bodies in Nigeria play a key role in minimizing fraudulent activities through audit mechanisms. The current study echoes this finding, as respondents indicated that audits by regulatory bodies help ensure compliance with fraud prevention measures. However, Olojede et al. (2020) highlighted that weak enforcement mechanisms can hinder the effectiveness of these audits, which is a point not fully addressed in this study, where respondents generally agreed on the effectiveness of regulatory audits and penalties.

Otieno (2021) emphasizes the importance of ethical compliance in reducing fraud, particularly among Kenyan professional accountants. This study aligns with Otieno's findings in that respondents agreed that employee training is a key part of ensuring compliance with fraud prevention policies. Both studies underscore the role of training in improving compliance and preventing fraudulent activities, with this study further highlighting that regulatory penalties are a deterrent. Wanjohi (2014) found that non-compliance with anti-money laundering (AML) policies contributed to fraud in Kenyan banks. The current study agrees with Wanjohi's findings, as respondents noted that their banks ensure regulatory compliance by adhering to such policies, and by having compliance officers who actively monitor and enforce these regulations. This study agrees with the findings of Clarke and Davison (2023), who emphasized that weak enforcement in international banks led to an increase in fraudulent activities. The study findings suggest that Kenyan banks, despite having regulatory compliance measures, may still face enforcement challenges in the practical implementation of these measures. Respondents expressed agreement that regulatory penalties help deter fraud, but this enforcement gap is an important issue to address in future research.

Akpan and Okafor (2023) explored regulatory compliance in Nigeria and highlighted the gaps in enforcement of compliance measures. Their findings contrast with the current study, where most respondents felt that regulatory compliance in Kenyan banks is

adequately enforced. While they noted that regulatory compliance in Kenya faces some challenges, the current study found strong agreement from employees on the effectiveness of fraud prevention measures and compliance efforts. Kinyanjui (2023) proposed integrating blockchain technology to improve fraud prevention mechanisms in Kenyan banks but did not address the practical challenges in implementing such technologies. The current study does not fully explore the role of blockchain or AI in strengthening regulatory compliance, though it does agree on the importance of collaboration with regulators to enhance fraud detection. Future studies should delve deeper into the practical barriers of integrating emerging technologies in Kenyan banks, as suggested by Kinyanjui (2023). The study by Oguejiofor et al. (2023) discussed the use of AI and data analytics to enhance regulatory compliance, but did not consider the ethical implications of using AI for fraud detection. This study did not fully explore the ethical concerns and privacy issues associated with using AI in regulatory compliance, which was a gap in the current research. This study focused on how regulatory bodies monitor and enforce policies but did not consider how these technologies may affect compliance efforts in Kenyan banks, particularly in relation to ethical considerations.

Deterrence Theory is relevant here, as the findings show that regulatory penalties act as a deterrent to fraudulent practices. The study emphasizes that effective enforcement of regulatory compliance through penalties and audits can deter fraud by increasing the perceived risk of engaging in fraudulent behavior, aligning well with the theory's emphasis on the role of perceived punishment in preventing crime.

5.3.3 Effect of organizational culture

The objective of this research was to examine how organizational culture influences fraudulent activities within Kenyan commercial banks. The results from this study showed that respondents agreed that the bank encourages ethical conduct, rewards individuals who follow ethical standards, and that management demonstrates exemplary behavior in preventing fraudulent activities. Additionally, respondents confirmed that employees can safely report suspicious activities without fear of retaliation and that there are strict penalties for fraudulent conduct. The study also revealed that employees endorse bank

transparency and financial accountability and support the strict anti-fraud policies and widespread training programs for ethical development.

The findings of this study agree with Rashid et al. (2022), who concluded that a strong ethical organizational culture is critical for fraud prevention. The study's emphasis on ethical conduct being encouraged and rewarded aligns with Rashid et al.'s assertion that a culture of honesty can significantly reduce fraudulent activities. This supports the idea that fostering a positive organizational culture can lead to more effective fraud mitigation in Kenyan banks. Both studies from Naivasha (2021) and Mwithi (2015) highlight that a culture promoting ethical behavior and integrity among employees helps in reducing fraud in Kenyan banks. These findings are consistent with this study, where respondents agreed that the bank promotes ethical behavior and integrity. Naivasha's research also emphasized the role of leadership in fostering such a culture, which resonates with the current study's findings that management sets a good example. These studies found that banks with strong ethical cultures experience fewer fraud incidents. The findings of this study agree with these studies, suggesting that the presence of a strong ethical culture in Kenyan banks can indeed reduce the likelihood of fraudulent activities. The study's emphasis on management setting good examples and transparency aligns with their findings.

While Rashid et al. (2022) emphasized the importance of ethical culture, they did not explore how employee engagement initiatives, such as participatory decision-making or team-building exercises, could enhance ethical behavior and reduce fraud. This study extends Rashid et al.'s findings by suggesting that such initiatives are crucial in fostering a positive culture within Kenyan banks, and future research should examine this relationship. Naivasha (2021) found that strategic management and an ethical culture significantly reduce fraud at Kenya Commercial Bank but did not explore the role of reward systems in reinforcing ethical behavior. This gap is addressed in this study, where it is suggested that rewards and penalties are essential components in encouraging ethical behavior and deterring fraud in Kenyan banks. While both studies underscore the importance of ethical leadership, they did not address the role of whistleblower protection policies in fostering an ethical culture. The current study fills this gap by emphasizing the

need for whistleblower protection to encourage employees to report unethical behavior safely and without fear of retaliation, which is crucial for reducing fraud in Kenyan banks. Although Dlamini and Khoza (2022) acknowledged the role of ethical training in curbing fraud, they did not assess the long-term impact of such training on reducing fraud, which remains a gap in the research. The present study also highlights the importance of sustained training and continuous employee development programs, which could lead to more permanent changes in the ethical culture of Kenyan banks.

The findings of this study are in agreement with Social Learning Theory (Sutherland, 1939; Akers, 1960), which suggests that behaviors, including fraudulent behavior, are learned through interactions with others within an individual's environment. By fostering an ethical organizational culture, Kenyan banks can reduce the likelihood of fraud being learned and replicated. Employees who observe ethical conduct and are positively reinforced for it are more likely to adopt similar behaviors, as predicted by Social Learning Theory.

5.3.4 Effect of technological advancements

This research aimed to examine how technological advancements influence fraud occurrence within Kenyan commercial banks. The findings revealed that the majority of respondents agreed that their bank utilizes advanced fraud detection technology to monitor transactions in real-time. They also agreed that cybersecurity measures are regularly updated to prevent fraud. Most respondents agreed that artificial intelligence (AI) and data analytics are employed to detect fraudulent activities and that online banking platforms are secure against fraudulent activities. Further, respondents agreed that technology adoption has significantly reduced fraud in their banks, and the study revealed that the bank continues to invest in continuous innovation to enhance fraud detection systems. Finally, respondents noted that employees are regularly trained on emerging fraud-related cybersecurity threats. The findings in this study agree with Rai and Acharya (2021), who emphasized the need for technological solutions, such as employee training and customer awareness, to mitigate fraud. This study extends their findings by also incorporating AI and data analytics as crucial technological tools in detecting fraudulent activities. Both studies highlight the increasing importance of integrating advanced technologies in fraud

prevention strategies in the banking sector. This study agrees with Hasham et al. (2019), who argued that cybersecurity integration with fraud prevention strategies is vital for managing emerging fraud risks. Like Hasham et al., this study finds that real-time transaction monitoring and AI-powered fraud detection systems are central to improving fraud prevention in Kenyan banks. The agreement between these studies supports the role of advanced analytics in enhancing fraud detection. The findings of this study align with the views of Wanjohi (2014) and Palshikar (2002), who emphasized the importance of advanced security measures such as firewalls and encryption. This study, however, extends their findings by introducing the concept of biometric authentication as a complementary tool to traditional security measures, thereby strengthening the fraud prevention framework. This research agrees with the studies of Tan and Wong (2023) and Sharma and Gupta (2022), who found that AI-driven tools and blockchain significantly improve fraud detection and financial security. The study's findings confirm that AI plays a critical role in identifying fraud and enhancing security systems within Kenyan banks. However, unlike these studies, this research also highlights the regulatory and ethical concerns related to the use of AI in fraud detection, a gap that needs further exploration.

While Rai and Acharya (2021) emphasized the need for employee training and customer awareness as part of fraud mitigation, they did not explore the integration of AI and data analytics in fraud detection. This study disagrees with that focus, as it found that AI and data analytics are crucial for detecting fraud in Kenyan banks, highlighting a more technology-driven approach to fraud prevention. Although Hasham et al. (2019) focused on cybersecurity, they did not address the specific role of AI-powered fraud detection systems. The findings of this study disagree with that gap by revealing that AI plays an essential role in identifying fraudulent transactions in Kenyan banks. This highlights a divergence between general cybersecurity measures and specific fraud detection technologies. While Wanjohi (2014) and Palshikar (2002) emphasized the importance of traditional security measures like firewalls and encryption, this study disagrees by suggesting that biometric authentication is an emerging technology that strengthens security and should complement traditional measures. Biometric authentication was not explored in their studies, but it was seen as an important tool in improving fraud detection in Kenyan banks. Oguejiofor et al. (2023) suggested that AI-driven technologies could

improve fraud detection but did not consider the ethical concerns related to implementing AI in regulatory compliance. The current study disagrees with this, as it highlights the privacy issues and algorithmic bias associated with the use of AI in fraud detection. Future research should explore how Kenyan banks can navigate these ethical and regulatory concerns while adopting AI.

Routine Activity Theory (Cohen & Felson, 1979) supports the study's findings by explaining how technological advancements can serve as capable guardians against fraud. The integration of AI and real-time transaction monitoring in Kenyan banks reduces the opportunity for fraud by increasing surveillance and identifying suspicious activities. The theory highlights the importance of reducing opportunities for fraud through improved technology, thus supporting the need for enhanced fraud detection systems.

5.3.5 Staff training

The objective of this research was to investigate how staff training influences the relationship between factors leading to fraudulent behavior within Kenyan commercial banking institutions. The study results showed that most participants agreed that employees receive regular training on fraud prevention and detection methods and that the bank provides periodic workshops on regulatory compliance combined with ethics. Additionally, they confirmed that employees are trained to use fraud detection technology and tools. Most respondents also agreed that employees are well-equipped to recognize and report fraudulent activities. Furthermore, they agreed that the training programs enhance employees' ability to adhere to internal control policies, and that fraud prevention training is tailored to specific roles within the bank. Finally, they noted that employees receive refresher courses on fraud prevention and compliance policies.

The findings from this study agree with Hamed (2023), who emphasized that staff training plays a crucial role in moderating the relationship between internal controls and fraud prevention in banks. The study found that well-trained employees are better equipped to detect fraud and comply with regulatory requirements, which strengthens fraud prevention strategies within the bank. The research findings align with Shwedeh and Rwashdeh (2022), who found that training employees on regulatory requirements and ethical standards significantly reduced fraud levels. This study concurs with the findings that

regular training in fraud prevention and compliance policies helps employees stay informed about fraud risks and adopt proactive fraud mitigation measures. The current study agrees with Bao et al. (2022), who highlighted the importance of integrating advanced technologies like AI and blockchain into training programs. The study showed that Kenyan bank employees need training to keep pace with technological advancements, a critical area where the current research agrees with Bao et al.'s findings. The study supports the views of Anindya and Adhariani (2022) and Zuberi and Mzenzi (2019) regarding the behavioral impact of training on employees' attitudes toward fraud prevention. The findings of the current study also suggest that fraud prevention training should be tailored to employees' roles and motivations to better shape ethical behavior. Supriadi (2024) recommended the integration of digital tools, such as AI, into fraud prevention training. This study agrees with Supriadi's suggestion and shows that training employees to adapt to new technological realities in fraud detection is a key focus in Kenyan banks.

While Shwede and Rwashdeh (2022) emphasized the importance of regulatory compliance training, their study did not address the long-term effectiveness of continuous training in keeping up with emerging fraud techniques. This study disagrees with that by indicating the need for ongoing and adaptive training programs to tackle new fraud challenges effectively, which is crucial as fraud techniques evolve. Although Bao et al. (2022) emphasized technological advancements, they did not explore how training programs could be adapted to meet the challenges posed by these evolving technologies. The current study disagrees by highlighting the need to integrate new technological tools such as AI and blockchain into staff training programs in Kenyan banks. Donnellan and Rutledge (2019) highlighted challenges faced by smaller banks in providing comprehensive fraud training, but they did not explore cost-effective training solutions for smaller institutions. The current study disagrees, emphasizing the importance of tailored, scalable training programs that can be accessed by all sizes of banks in Kenya, thus ensuring a more uniform approach to fraud prevention.

Fraud Triangle Theory suggests that staff training can help reduce the opportunity for fraud by improving internal controls and enhancing employees' ability to detect fraud. The

training programs, particularly those focused on fraud detection tools, address the opportunity and rationalization elements of the fraud triangle. By equipping employees with the necessary skills, training helps reduce the opportunity for fraud and promotes ethical behavior, thus moderating the relationship between the factors that contribute to fraudulent activities.

5.4 Conclusion

This study provides significant new insights into the dynamics of fraudulent practices within Kenyan commercial banks, specifically emphasizing the moderating role of staff training in enhancing the effectiveness of fraud prevention strategies. The findings reveal that while traditional fraud prevention measures—such as internal control systems, regulatory compliance, organizational culture, and technological advancements—are effective, staff training serves as a crucial moderator that significantly enhances these measures' predictive power and effectiveness.

The Fraud Triangle Theory is strongly supported by the data, as the results show that internal control systems, regulatory compliance, organizational culture, and technological advancements all contribute significantly to reducing fraudulent practices among employees. The study specifically highlights that staff training moderates these relationships, increasing the explanatory power of these variables. The results show that staff training not only strengthens the impact of internal controls but also influences regulatory compliance and organizational culture in reducing fraud. Interestingly, the study also found that the moderating effect of staff training on regulatory compliance had a negative impact on fraud prevention, suggesting that training may highlight the need for more tailored compliance efforts rather than just blanket adherence to regulations.

The research offers novel findings by demonstrating that staff training directly impacts how employees engage with and utilize internal controls, the ethical culture of the organization, and the technological tools available to them. Specifically, the training enhanced the effectiveness of internal controls and improved employee response to fraud detection technologies, while simultaneously strengthening the organizational culture in combating fraud. These findings align with Social Learning Theory, showing that

employees are less likely to engage in fraudulent activities when they are properly trained to understand ethical standards and the consequences of fraud.

Furthermore, Routine Activity Theory is validated by the study's evidence that technological advancements in fraud detection, combined with staff training, create a more robust environment for preventing fraud. Trained employees act as effective guardians, ensuring that routine banking activities, such as transactions and loan handling, are consistently monitored and protected against fraudulent actions.

A key contribution of this research is the demonstration that staff training is not just a supplementary measure but an integral factor that significantly moderates the impact of internal controls, regulatory compliance, organizational culture, and technological advancements. The data reveals that staff training contributes an additional 3.2% to the explained variance in fraud occurrence when incorporated with internal controls, regulatory compliance, and organizational culture. This is a critical finding that underscores the importance of ongoing employee education as a core component of fraud prevention strategies.

The study's findings suggest that Kenyan commercial banks, while already implementing internal controls, compliance measures, and technology, must focus on strengthening staff training programs. Training programs should be tailored to enhance employees' ability to understand and engage with fraud prevention mechanisms, ensuring that these systems are fully optimized in day-to-day operations. Moreover, the findings suggest that more attention should be paid to how staff training can influence regulatory compliance efforts and improve adherence to ethical standards, further preventing fraud within banks.

This research contributes new knowledge by highlighting the moderating effect of staff training on fraud prevention, an area that has been underexplored in the literature. The results underscore that staff training is essential for ensuring the optimal functioning of existing fraud prevention systems. The study's innovative contribution lies in showing how training programs can enhance the interaction between internal controls, regulatory compliance, organizational culture, and technology, resulting in a more integrated and robust approach to fraud prevention. These findings have important implications for the

design of training programs in Kenyan banks, suggesting that banks should invest in continuous training that not only focuses on compliance but also on fostering a proactive and ethical culture among employees.

5.5 Recommendations of the study

Based on the study findings, the study made the following recommendations:

To enhance the effectiveness of internal control systems in Kenyan commercial banks, it is recommended that banks integrate advanced digital risk management tools, such as AI-powered transaction monitoring, to better detect and address emerging fraud risks. Additionally, targeted training programs should be developed to ensure employees not only understand but can effectively apply internal controls in their day-to-day operations. Banks should also revisit their segregation of duties and enhance oversight mechanisms, ensuring that weak spots are identified and addressed to reduce opportunities for fraud. This combination of advanced technology, practical training, and stronger oversight will fortify internal control systems and prevent fraudulent behavior.

For regulatory compliance to be more effective in preventing fraud, Kenyan banks should adopt a risk-based regulatory compliance framework that targets high-risk areas based on fraud severity. This approach ensures better allocation of resources and adaptable strategies to combat fraud. Further, integrating technological solutions like AI and blockchain into compliance monitoring will help banks stay ahead of fraud risks in real-time. It is also important for Kenyan banks to continue strengthening their collaboration with regulators, ensuring that feedback and audit recommendations are swiftly implemented, while also addressing practical challenges in enforcement through targeted solutions.

To foster a more ethical organizational culture, Kenyan banks should focus on strengthening ethical leadership and holding senior management accountable for setting a good example. In addition to promoting ethical behavior, employee engagement initiatives, such as participatory decision-making and team-building exercises, should be implemented to deepen employees' investment in the bank's ethical culture. Banks should also strengthen whistleblower protection policies to encourage employees to report

unethical behavior without fear of retaliation. These measures, when integrated, will promote a positive organizational culture that actively discourages fraudulent activities.

Kenyan banks should invest in cutting-edge technologies, such as biometric authentication systems and AI-driven fraud detection tools, to enhance the security of online banking platforms and reduce the risk of fraud. Additionally, integrating predictive analytics into fraud prevention strategies will allow banks to identify and address potential fraud before it occurs. It is also essential for banks to continuously update their cybersecurity measures and provide staff training on emerging threats, ensuring that employees are well-equipped to handle new fraud risks in the digital banking landscape.

Staff training should be role-specific and tailored to the unique fraud risks faced by different bank employees. This will ensure that frontline staff, compliance officers, and managers are equipped with the necessary tools to detect and prevent fraud effectively. Additionally, incorporating advanced technologies, such as AI and blockchain, into training programs will ensure employees remain proficient in using new fraud detection tools. Finally, training should also address the behavioral aspects of fraud prevention, focusing on ethics and compliance motivation, to help employees understand the importance of upholding ethical standards in the workplace and reduce the rationalization of fraudulent behavior.

5.6 Limitation of the study

Limitation of this study is that the use of primary data collected using questionnaires makes it difficult to ascertain the truth of the information provided by respondents. Bias from socially desirable responses is a potential limitation. Besides methodological limitations, conceptual limitations existed in this research. In particular, this study only focused on commercial banks in Kenya.

5.7 Suggestion for the study

Additional investigation of employee behaviors coupled with individual ethical awareness should follow this study since it focuses on organizational culture and ethical behavior prevention of fraud. The understanding of workplace factors which influence employee conduct regarding fraud would benefit from better knowledge of employee satisfaction

levels as well as personal values and ethical work environments. Understanding individual-level ethical decision-making factors will enable banks to design superior ethical training as well as policies to build an ethical and watchful organizational culture.

The research proved the bank has implemented whistleblowing systems yet more investigation would measure their capacity to stop and detect fraudulent activities. The evaluation of reporting process safety perceptions and employee system trust and management whistleblower response abilities would show which factors lead employees to choose or avoid whistleblowing channels. A comprehensive analysis of these factors enables bank managers to develop strong whistleblowing systems while protecting staff who report corruption from any workplace reprisals.

Real-time monitoring systems along with artificial intelligence and data analytics represent key technological developments that prove effective for lowering cases of fraud according to this piece of research. Future investigations should study how blockchain technology and machine learning applications might help achieve more effective fraud prevention. Research on bank daily operations integration and fraud detection accuracy effects from these technologies will deliver significant findings to banking institutions.

5.8 Chapter summary

Chapter 5 summarizes the findings from the study, presents the conclusions from the data and provides recommendations for addressing fraudulent practices in Kenyan commercial banks. Additionally, the chapter suggests areas for further research to expand on the findings of this study. The study found that most respondents agreed that their banks have effective internal control systems to prevent fraudulent activities. Effect of Regulatory Compliance the respondents reveals that majority of respondents agreed that their banks comply with all regulatory requirements related to fraud prevention.

Organizational culture was another significant factor in fraud prevention, according to the study's findings. Technological advancements were found to be a major factor in fighting fraud. The study concluded that several factors play a critical role in preventing fraudulent activities in Kenyan commercial banks. Strong internal control systems, regulatory compliance, organizational culture, technological advancements, and staff training were

identified as key components of effective fraud prevention. Internal control systems, including regular risk assessments and clearly defined employee roles, were found to be crucial in mitigating fraud risks. Regulatory compliance, which includes audits, training and penalties, also helps reduce fraud.

Based on the findings, the study made several recommendations for Kenyan commercial banks to enhance their fraud prevention efforts. First, banks should strengthen their whistleblowing systems to encourage better participation from employees in reporting fraudulent activities. The study suggests several areas for further research. One suggestion is to investigate employee behaviors and ethical awareness, specifically examining how workplace factors like employee satisfaction and personal values influence fraud prevention efforts.



REFERENCES

- Abei, Y. A. (2021). Impact of internal control on fraud detection and prevention in microfinance institutions.
- Abiola, I., & Oyewole, A. T. (2013). Internal Control System on Fraud Detection: Nigeria Experience. *Journal of Accounting and Finance*, 13(5), 137-148.
- Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Reviewing Third-Party Risk Management: Best Practices in Accounting and Cybersecurity for Superannuation Organizations. *Finance & Accounting Research Journal*, 6(1), 21-39.
- Abu Amuna, Y. M., & Abu Mouamer, F. (2020). Impact of applying fraud detection and prevention instruments in reducing occupational fraud: case study: ministry of health (MOH) in Gaza Strip. *International Journal of Advanced Studies of Scientific Research*, 4(6).
- Adegbite, E., Olayemi, O., & Akinmoladun, F. (2021). The impact of internal control systems on fraud in Nigerian banks. *African Journal of Business Management*, 15(10), 456-470.
- Adekunle, O., & Olusa, A. (2021). The Impact of Fraudulent Practices on Infrastructural Development in Nigeria. *J Econ Sustainable Dev*, 12(6), 81-89.
- Adeoye, O. B., Addy, W. A., Odeyemi, O., Okoye, C. C., Ofodile, O. C., Oyewole, A. T., & Ololade, Y. J. (2024). Fintech, Taxation, And Regulatory Compliance: Navigating the New Financial Landscape. *Finance & Accounting Research Journal*, 6(3), 320-330.
- Adeyemo, K., & Obafemi, F. J. (2024). A survey on the role of technological innovation in Nigerian deposit money bank fraud prevention. *South Asian Journal of Social Studies and Economics*, 21(3), 133-150.
- Aguilera, R. V., & Cuervo-Cazurra, A. (2009). Codes of good governance. *Corporate Governance: An International Review*, 17(3), 376–387. <https://doi.org/10.1111/j.1467-8683.2009.00737.x>
- Ahmed, A. F., & Rugami, M. (2019). Corporate Governance and Performance of Savings and Credit Cooperative Societies in Kilifi County, Kenya. *International Academic Journal of Economics and Finance*, 3(3), 61-79.
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024). Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation. *Journal of Financial Crime*, 31(1), 201-225.
- Akpan, U., & Okafor, M. (2023). The effectiveness of Central Bank regulations in fraud prevention in Nigerian banks. *Journal of Banking and Finance*, 39(4), 112-128.

- AL-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, 15(1), 1315-1331.
- Al-Mamun, A., Rashid, M. A., & Yasser, Q. R. (2020). Corporate governance and fraud prevention in financial institutions: A cross-jurisdictional study. *Journal of Financial Crime*, 27(3), 745-760.
- Aman-Ullah, A., & Mehmood, W. (2023). Role of Islamic work ethics in shaping employees' behaviour: evidence from the banking sector in Azad Jammu and Kashmir. *Journal of Islamic Accounting and Business Research*, 14(7), 1033-1047.
- Ametepe, P. K., Banwo, A. O., & Arilesere, M. S. (2023). Amoral behavior, control climate, job insecurity and fraudulent intentions among bank employees. *International Journal of Ethics and Systems*, 39(4), 781-803.
- Ammirato, S., Sofo, F., Felicetti, A. M., & Raso, C. (2019). A Methodology to Support the Adoption of Iot Innovation and Its Application to The Italian Bank Branch Security Context. *European Journal of Innovation Management*, 22(1), 146-174.
- Anindya, J. R., & Adhariani, D. (2019). Fraud Risk Factors and Tendency to Commit Fraud: Analysis of Employees' Perceptions. *International Journal of Ethics and Systems*, 35(4), 545-557.
- Anyona, V. O. (2024). Effect Of Corporate Governance On Fraud Mitigation Among Microfinance Banks In Kenya (Doctoral dissertation, KCA University).
- Archer, R. J. L., & Flexon, J. L. (2022). Unstructured socializing with peers and delinquency: The role of mediation through the lens of Akers'(1998) social structure social learning theory of crime and deviance. *American Journal of Criminal Justice*, 47(5), 980-1005.
- Arjoon, S. (2006). Striking a balance between rules and principles-based approaches for effective governance: A risks-based approach. *Journal of Business Ethics*, 68(1), 53–82. <https://doi.org/10.1007/s10551-006-9040-6>
- Assidi, S. (2020). The Effect of Voluntary Disclosures and Corporate Governance on Firm Value: A Study of Listed Firms in France. *International Journal of Disclosure and Governance*, 17(2), 168-179.
- Association of Certified Fraud Examiners. (2021). Report to the Nations: 2021 Global Study on Occupational Fraud and Abuse. Austin, TX: ACFE.
- Awalluddin, M. A., Nooriani, T. I. T., & Maznorbalia, A. S. (2022). The Relationship Between Perceived Pressure, Perceived Opportunity, Perceived Rationalization and Fraud Tendency Among Employees: A Study from the People's Trust in Malaysia. *Studies in Business & Economics*, 17(2).

- Awodiran, M. A. (2022). Determinants Of Financial Reporting Fraud Among Listed Non-Financial Firms in Nigeria (Doctoral Dissertation, Kwara State University (Nigeria)).
- Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110-132.
- Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110-132.
- Aziz, L. A., & Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Journal of Banking and Financial Technology*, 2(2), 130-145.
- Bao, Y., Hilary, G., & Ke, B. (2022). Artificial Intelligence and Fraud Detection. *Innovative Technology at The Interface of Finance and Operations: Volume I*, 223-247.
- Barker, R. (2018). Knowledge management to prevent fraudulent e-banking transactions. *Communitas*, 23, 71-86.
- Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 51(6), 1173–1182. <https://doi.org/10.1037/0022-3514.51.6.1173>
- Baten, M. A. (2020). Basic understanding of fraudulent activities in corporate organisation. *Review of Business, Accounting, & Finance*, 1(01), 1-13.
- Bello, O. A., & Olufemi, K. (2024). Artificial Intelligence in Fraud Prevention: Exploring Techniques and Applications Challenges and Opportunities. *Computer Science & IT Research Journal*, 5(6), 1505-1520.
- Berkovich, I. (2018). Beyond qualitative/quantitative structuralism: The positivist qualitative research and the paradigmatic disclaimer. *Quality & Quantity*, 52(5), 2063–2077.
- Bhaskar, R. (2008). *A realist theory of science*. Verso.
- Bhat, S. (2023). The Effectiveness of Internal Controls in Preventing Fraud and Financial Misconduct. *Journal Of Law and Sustainable Development*, 11(5), E1178-E1178.

- Bhatt, S., Kumar, V., & Kumar, S. (2023, April). Analyzing Frauds in Banking Sector and Impact of Internet Banking on Its Customers: A Case Study of Bank of Maharashtra. In *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)* (Pp. 178-182). IEEE.
- Bishop, D. Y. (2022). *Fraud Risk Management to Detect and Prevent Employee Fraud in Small Rural Businesses*. Liberty University.
- Blair, J., & Barbiani, M. (2019). *Regulatory Compliance and Fraud Prevention in Banking*. *Journal of Financial Crime*, 26(3), 721–735. <https://doi.org/10.1108/JFC-11-2018-0123>
- Blair, W., & Barbiani, C. (2019). Ethics and standards in financial regulation. In *Research handbook on law and ethics in banking and finance* (pp. 25-54). Edward Elgar Publishing.
- Boone, H. N., & Boone, D. A. (2012). Analyzing Likert data. *Journal of Extension*, 50(2), 1–5.
- Brazhkin, V. (2020). “I have just returned from the moon:” online survey fraud. *Supply Chain Management: An International Journal*, 25(4), 489-503.
- Brown, D., Batra, G., Zafar, H., & Saeed, K. (2024). Reducing fraud in organizations through information security policy compliance: An information security controls perspective. *Computers & Security*, 144, 103958.
- Brown, D., Batra, G., Zafar, H., & Saeed, K. (2024). Reducing fraud in organizations through information security policy compliance: An information security controls perspective. *Computers & Security*, 144, 103958.
- Bryant, C. G. A. (1985). *Positivism in Social Theory and Research*. Springer.
- Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.
- Central Bank of Kenya. (2020). *Banking sector fraud report*. Nairobi: Central Bank of Kenya.
- Central Bank of Kenya. (2022). *Kenya Financial Stability Report*. Nairobi: Central Bank of Kenya.
- Central Bank of Kenya. (2023). *Annual Report on Banking Fraud*.
- Challapalli, S. (2023). Benefits And Constraints Associated with The Harmonization of Financial Regulations: An Overview. *Asian Journal of Economics, Business and Accounting*, 23(15), 49-56.
- Chege, J. (2021). *Digital Banking and Security Measures in Kenya: A Policy Review*. Nairobi: Kenya Policy Review Association.

- Chege, S., & Mutua, D. (2019). Internal Fraud in Kenyan Banks: Organizational Culture and Employee Conduct, Kenya. *Journal of Banking and Finance*, 33(3), pp. 45-60.
- Chen, J., & Elder, S. (2021). Internal controls and fraud prevention in U.S. commercial banks. *Journal of Financial Crime*, 28(2), 65-78.
- Chiezey, U., & Onu, A. J. C. (2013). Impact of Fraud and Fraudulent Practices on the Performance of Banks in Nigeria. *British Journal of Arts and Social Sciences*, 15(1), 12-25.
- Chitai, W., Wangari, L., Kamau, B., & Mutua, J. (2024). E-Banking Strategies and Financial Performance of Commercial Banks in Kenya. *Finance and Accounting*, 9(2), 62-80.
- Choi, J. H., & Gipper, B. (2024). Fraudulent financial reporting and the consequences for employees. *Journal of Accounting and Economics*, 78(1), 101673.
- Cholisoh, L., & Hadziq, M. F. (2021). Implementation of GCG (Good Corporate Governance) on the Prevention of Fraud Financing in Islamic Banks. *El-Qish: Journal of Islamic Economics*, 1(2), 98-108.
- Cinaj, V., Meçe, M. A. N. U. E. L. A., Ribaj, A., & Kadrimi, I. (2020). The need for improvement of external audit reports of banks (the case of banks in Albania which mainly belong to EU Banks). *WSEAS Transactions on Business and Economics*, 17, 539-547.
- Clarke, A., & Davison, T. (2023). Compliance failures and their role in banking fraud. *Financial Institutions Review*, 33(1), 145-159.
- Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/correlation analysis for the behavioral sciences* (3rd ed.). Routledge.
- Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal Control—Integrated Framework. COSO.
- COSO (Committee of Sponsoring Organizations of the Treadway Commission). (2013). *Internal Control — Integrated Framework*. COSO.
- Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
- Daoud, J. I. (2017). Multicollinearity and regression analysis. *Journal of Physics: Conference Series*, 949, 1–6. <https://doi.org/10.1088/1742-6596/949/1/012009>
- Debbarma, R. (2023). The Legal Framework And Challenges In Prosecuting Cybercrimes Including Hacking, Identity Theft, And Online Fraud. *resmilitaris*, 13(2), 7021-7048.

- DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2020). Financial fraud among older Americans: Evidence and implications. *The Journals of Gerontology: Series B*, 75(4), 861-868.
- Denscombe, M. (2014). *The good research guide: For small-scale social research projects* (5th ed.). Open University Press.
- DeZoort, F. T., & Harrison, P. D. (2018). Understanding auditors' sense of responsibility for detecting fraud within organizations. *Journal of business ethics*, 149, 857-874.
- Dlamini, T., & Khoza, P. (2022). The role of corporate governance and ethical behavior in preventing financial fraud in South Africa. *South African Journal of Business Ethics*, 14(2), 45-59.
- Donnellan, J., & Rutledge, W. L. (2019). A Case for Resource-Based View and Competitive Advantage in Banking. *Managerial And Decision Economics*, 40(6), 728-737.
- Dorminey, J., Fleming, A. S., Kranacher, M.-J., & Riley, R. A. (2012). The Fraud Triangle: Introducing an Additional Dimension. *Journal of Forensic Accounting Research*, 7(1), 17–39. <https://doi.org/10.2308/jfar-10209>
- European Central Bank. (2022). Annual Report on Financial Crimes.
- Federal Reserve. (2022). Report on Cybersecurity and Financial Fraud.
- Federal Reserve. (2023). Cybersecurity in Financial Institutions. Washington, D.C.: Federal Reserve.
- Fernandhytia, F., & Muslichah (2020). The effect of internal control, individual morality, and ethical value on accounting fraud tendency. *Media Ekonomi dan Manajemen*, 35(1), 112-127.
- Financial Conduct Authority. (2022). Annual Report on Fraud and Cybercrime. London: FCA.
- Ghanem, M. G., & Awad, G. (2023). The Impact of Internal Control Systems on Minimizing Fraud: The Case of Lebanon. *European Journal of Business and Management Research*, 8(5), 69-75.
- Gonzalez, G. C., & Hoffman, V. B. (2018). Continuous auditing's effectiveness as a fraud deterrent. *Auditing: A Journal of Practice & Theory*, 37(2), 225-247.
- Gonzalez, G. C., & Hoffman, V. B. (2018). Continuous auditing's effectiveness as a fraud deterrent. *Auditing: A Journal of Practice & Theory*, 37(2), 225-247.

- Grandstaff, J. L., & Solsma, L. L. (2021). Financial statement fraud: a review from the era surrounding the financial crisis. *Journal of Forensic and Investigative Accounting*, 13(3), 421-437.
- Grilli, L., & Rampichini, C. (2021). An introduction to ordinal logistic regression. *Journal of Modern Applied Statistical Methods*, 20(1), 101–113. <https://doi.org/10.22237/jmasm/1617631860>
- Gulyas, O., & Kiss, G. (2023). Impact Of Cyber-Attacks on Financial Institutions. *Procedia Computer Science*, 219, 84-90.
- Gutterman, A. S. (2023). Training and development. Available at SSRN 4555407.
- Hadian, N., Rufaidah, A. N., Vionica, V., Avionita, D., Ibrahim, I., Zumar, A., & Sinaga, O. (2021). The Effect Of Internal Control On Fraud Detection (Case Study On Several State-Owned Enterprises Banks In Bandung City). *Review of International Geographical Education Online*, 11(5), 1059-1064.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate data analysis* (7th ed.). Pearson Education Limited.
- Hamed, R. (2023). The Role of Internal Control Systems in Ensuring Financial Performance Sustainability. *Sustainability*, 15(13), 10206.
- Hammersley, M. (2019). *What is positivism?* Routledge. <https://doi.org/10.4324/9781315145167>
- Handoyo, B. R. M., & Bayunitri, B. I. (2021). The Influence of Internal Audit and Internal Control Toward Fraud Prevention. *International Journal of Financial, Accounting, And Management*, 3(1), 45-64.
- Hardika, A. L., & Lubis, D. M. A. S. (2021). Fraud Prevention Measures at PT. Bank BJB, Bandung City. *Turkish Journal of Computer and Mathematics Education*, 12(9), 118-122.
- Hasan, M. N. (2016). Positivism: To what extent does it aid our understanding of the contemporary social world? *Quality & Quantity*, 50(1), 317–325
- Hasan, Z., Saifunnajar, S., Azlina, N., Al Mansur, M., & Saifullah, S. (2022). Implementation of whistleblowing system to prevent sharia banking crime in Indonesia. *AZKA International Journal of Zakat & Social Finance*, 32-52.
- Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity*. McKinsey & Company.
- Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). The risk of financial fraud: a management perspective. *Journal of Financial Crime*, 27(4), 1143-1159.

- Hassan, S. W. U., Kiran, S., Gul, S., Khatatbeh, I. N., & Zainab, B. (2025). The perception of accountants/auditors on the role of corporate governance and information technology in fraud detection and prevention. *Journal of Financial Reporting and Accounting*, 23(1), 5-29.
- Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (2nd ed.). Guilford Press.
- Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-Based Nursing*, 18(3), 66–67. <https://doi.org/10.1136/eb-2015-102129>
- Henson, B. (2020). Routine Activities. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 469-489.
- Hidayah, I., Pramono, S. E., & Sutopo, Y. (2024). How effective leadership mediates the influence of organizational culture, governance, and integrity on employee performance. *Journal of Ecohumanism*, 3(8), 1617-1650.
- Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*.
- Hoai, T. T., Hung, B. Q., & Nguyen, N. P. (2022). The Impact of Internal Control Systems on The Intensity of Innovation and Organizational Performance of Public Sector Organizations in Vietnam: The Moderating Role of Transformational Leadership. *Heliyon*, 8(2).
- Huang, X., Liu, F., & Zhang, Y. (2022). Cybersecurity and Fraud Prevention in Chinese Banks. *Journal of Financial Crime*, 19(1), 112-130.
- Igbojiyibo, R. P. (2024). The Impact of Internal Control Systems on Asset Protection and Financial Reporting Accuracy in Smes. *Asian Journal of Economics, Business and Accounting*, 24(12), 65-80.
- Ikhsan, W. M., Ednoer, E. H., Kridantika, W. S., & Firmansyah, A. (2022). Fraud detection automation through data analytics and artificial intelligence. *Riset: Jurnal Aplikasi Ekonomi Akuntansi dan Bisnis*, 4(2), 103-119.
- Ilugbusi, S., Olulade, K. A., & Awoniyi, C. O. (2020). Impact of internal control on fraud prevention in deposit money banks in Nigeria. *Nigerian Studies in Economics and Management Sciences*, 2(1), 42-51.
- International Monetary Fund. (2021). *Global Financial Stability Report*. Washington, D.C.: IMF.
- Jensen, M. C., & Meckling, W. H. (1919). Theory Of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. In *Corporate Governance* (Pp. 77-132). Gower.

- Jones, M., & Patterson, R. (2022). Organizational culture and its impact on fraud prevention in multinational banks. *Journal of Business Ethics*, 48(6), 99-112.
- Jones, R. W., & Pridemore, W. A. (2019). Toward An Integrated Multilevel Theory of Crime at Place: Routine Activities, Social Disorganization, And the Law of Crime Concentration. *Journal Of Quantitative Criminology*, 35, 543-572.
- Kagias, P., Cheliatsidou, A., Garefalakis, A., Azibi, J., & Sariannidis, N. (2022). The fraud triangle—an alternative approach. *Journal of Financial Crime*, 29(3), 908-924.
- Kamal, M., Alam, M. R., & Rahmani, S. (2025). Evaluating the Regulatory Framework for Bank Fraud Prevention in India: Effectiveness and Suggested Improvements. *Available at SSRN 5113109*.
- Kamau, A., & Were, M. (2018). What drives banking sector performance in Kenya? *Global Business and Economics Review*, 20(1), 1–15.
- Kamau, P., & Otieno, J. (2022). Internal control systems and fraud in Kenyan commercial banks. Kenya. *Journal of Business Studies*, 8(4), 112-129.
- Kamau, S., & Mutua, J. (2022). Trends in banking fraud in East Africa. *Journal of Financial Crime*, 29(2), 504-521.
- Kaptein, M. (2011). Understanding Unethical Behavior by Unraveling Ethical Culture. *Human Relations*, 64(6), 843–869. <https://doi.org/10.1177/00187267110390536>
- Kariuki, M. W., & Muturi, W. (2015). Factors affecting performance of commercial banks in Nairobi County: A case study of National Bank of Kenya. *International Journal of Economics, Commerce and Management*, 3(4), 1–15.
- Kariuki, N., & Wanjiru, R. (2023). Cybersecurity threats and digital fraud detection mechanisms in Kenyan banks. *Cybersecurity Review*, 15(2), 105-119.
- Kariuki, S., & Wanjohi, P. (2018). Cybersecurity risks in Kenyan banks: A case study of mobile banking. *Journal of Information Security*, 9(3), 123–135. <https://doi.org/10.4236/jis.2018.93010>
- Kashona, S. (2019). The effectiveness of internal control and internal audit in fraud detection and prevention: A case study of Ministry of Finance-Namibia (Doctoral dissertation, University of Namibia).
- Kassambara, A. (2018). Practical guide to regression analysis in R. STHDA.
- Kassem, R. (2022). Elucidating corporate governance’s impact and role in countering fraud. *Corporate Governance: The International Journal of Business in Society*, 22(7), 1523-1546.

- Kaur, B., Sood, K., & Grima, S. (2023). A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance*, 31(1), 60-95.
- Kaur, G., Singh, P., & Sharma, R. (2023). The Role of Staff Training in Enhancing Fraud Detection and Prevention: A Banking Sector Perspective. *International Journal of Bank Marketing*, 41(2), 230–247. <https://doi.org/10.1108/IJBM-06-2022-0311>
- Kim, H. Y., Park, H., & Lee, S. (2015). Basic statistical tests for assessing normality and variability: A guide for non-statisticians. *Korean Journal of Anesthesiology*, 68(6), 540–546. <https://doi.org/10.4097/kjae.2015.68.6.540>
- Kimani, J., & Kibera, M. (2023). Evolution of risks facing commercial banks in Kenya and associated strategic responses. *International Journal of Modern Risk Management*, 1(2), 56-65.
- Kinyanjui, A. (2023). Blockchain technology and regulatory compliance in Kenyan banks. *Kenya Financial Innovation Journal*, 12(1), 35-47.
- Kipchumba, S., & Magutu, P. O. (2013). Fraud risk management in Kenyan commercial banks. *Journal of Financial Crime*, 20(3), 271–283. <https://doi.org/10.1108/JFC-03-2013-0018>
- Kiplagat, R. (2021). Predictive Analytics in Fraud Prevention: A Case Study of Kenyan Commercial Banks. *African Journal of Information Systems*, 13(4), pp. 237-253.
- Kiplangat, J., Juma, D., & Omagwa, J. (2019). Effect of bank characteristics on financial performance of commercial banks in Kenya. *International Journal of Current Aspects*, 3(6), 28–41.
- Koech, S. K. (2019). The Effects of Corruption as An Economic Crime on Economic Growth and Implications on National Security in Kenya, 2005-2016 (Doctoral Dissertation, University of Nairobi).
- Kokogho, E., Onwuzulike, O. C., Omowole, B. M., Ewim, C. P. M., & Adeyanju, M. O. (2025). Blockchain technology and real-time auditing: Transforming financial transparency and fraud detection in the Fintech industry. *Gulf Journal of Advance Business Research*, 3(2), 348-379.
- KPMG. (2021). Kenya Banking Sector Fraud Survey. Nairobi: KPMG Kenya.
- Krishnakumar, A., & Verma, S. (2021). Understanding Domestic Violence in India During COVID-19: A Routine Activity Approach. *Asian Journal of Criminology*, 16(1), 19-35.
- Kumar, K., Bhattacharya, S., & Hicks, R. (2018). Employee Perceptions of Organization Culture with Respect to Fraud—Where to Look and What to Look For. *Pacific Accounting Review*, 30(2), 187-198.

- Kuraku, D. S., Kalla, D., & Samaah, F. (2022). Navigating The Link Between Internet User Attitudes and Cybersecurity Awareness in The Era of Phishing Challenges. *International Advanced Research Journal in Science, Engineering and Technology*, 9(12).
- Kurum, E. (2023). Regtech Solutions and AML Compliance: What Future for Financial Crime? *Journal Of Financial Crime*, 30(3), 776-794.
- Kuruppu, C. L., Kavirathne, C. S., & Karunarathna, N. (2021). The impact of training on employee performance in a selected apparel sector organization in Sri Lanka.
- Lau, A. C. Y. (2024). *Applying the fraud triangle theory to examine fraudulent cases from the perspective of working adult* (Doctoral dissertation, UTAR).
- Lau, A. C. Y. (2024). Applying The Fraud Triangle Theory to Examine Fraudulent Cases from The Perspective of Working Adult (Doctoral Dissertation, UTAR).
- Le, N. T., Vu, L. T., & Nguyen, T. V. (2021). The use of internal control systems and codes of conduct as anti-corruption practices: evidence from Vietnamese firms. *Baltic Journal of Management*, 16(2), 173-189.
- Lederman, L. (2019, January). The Fraud Triangle and Tax Evasion. In *Proceedings. Annual Conference on Taxation and Minutes of The Annual Meeting of The National Tax Association* (Vol. 112, Pp. 1-54). National Tax Association.
- Liu, Q., & Zhang, L. (2023). Ethical leadership and transparency in banking: A comparative study. *Journal of Financial Ethics*, 6(2), 110-123.
- Loeb, S., Dynarski, S., McFarland, D., Morris, P., Reardon, S., & Reber, S. (2017). Descriptive analysis in education: A guide for researchers. *National Center for Education Evaluation and Regional Assistance*.
- Lourens, L. (2021). Assessing the impact of internal control systems on financial performance and fraud management in South African banks. *Journal of Financial Crime*, 18(4), 400-415.
- Mabunda, S. (2024). Applying the Routine Activities Theory to Cybercrime: A Cyber-Capable Guardian. *JACL*, 8, 60.
- Martins, O. S., & Ventura Júnior, R. (2020). The Influence of Corporate Governance on The Mitigation of Fraudulent Financial Reporting. *Revista Brasileira De Gestão De Negócios*, 22, 65-84.
- Maulidi, A., & Ansell, J. (2021). Tackling practical issues in fraud control: a practice-based study. *Journal of Financial Crime*, 28(2), 493-512.

- McGrath, J., & Walker, C. (2023). Regulating ethics in financial services: Engaging industry to achieve regulatory objectives. *Regulation & Governance*, 17(3), 791-809.
- Mochere, S. N. (2020). Money Laundering in The Banking Sector: A Critical Analysis of The Enforcement Procedures in Kenya (Doctoral Dissertation, Strathmore University).
- Moirangthem, S., Olivier, C., Gagneux-Brunon, A., Péllissier, G., Abiteboul, D., Bonmarin, I., ... & Mueller, J. E. (2022). Social conformism and confidence in systems as additional psychological antecedents of vaccination: a survey to explain intention for COVID-19 vaccination among healthcare and welfare sector workers, France, December 2020 to February 2021. *Eurosurveillance*, 27(17), 2100617.
- Molefe, T., & Mkhize, N. (2023). The role of internal controls in reducing fraud in South African financial institutions. *South African Financial Review*, 20(1), 58-74.
- Montgomery, D. C., Peck, E. A., & Vining, G. G. (2012). *Introduction to linear regression analysis* (5th ed.). Wiley.
- Mose, J., & Korir, M. (2020). Impact of Digital Banking on Fraud in East African Banks. *East African Financial Review*, 6(2), 158-174.
- Mulugeta, W. (2021). The Effectiveness Of Internal Control System For Detection And Prevention Of Fraud The Case Of Selected Commercial Banks In Ethiopia (Doctoral Dissertation, St. Mary's University).
- Muntahanah, S., Kusuma, H., Harjito, D. A., & Arifin, Z. (2021). The Effect of Family Ownership and Corporate Governance on Firm Performance: A Case Study in Indonesia. *The Journal of Asian Finance, Economics and Business*, 8(5), 697-706.
- Muthinja, M. M., & Chipeta, C. (2018). What drives financial innovations in Kenya's commercial banks? An empirical study on firm and macro-level drivers of branchless banking. *Journal of African Business*, 19(3), 385-408.
- Mwai, R., Wabala, S., & Ogada, K. (2023). Role of ICT Risk Management on Insider Fraud Prevention in Commercial Banks in Nairobi County. *International Journal of Technology and Systems*, 8(2), 36-64.
- Mwangi, A. W. (2022). Determinants Of Effective Fraud Risk Management Practices Among Medical Insurance Providers in Kenya (Doctoral Dissertation, Strathmore University).
- Mwangi, C., & Kimani, G. (2023). The role of ethical behavior in fraud prevention in Kenyan banks. *Kenya Business Ethics Journal*, 7(3), 54-69.

- Mwangi, L. W., & Ouma, S. A. (2012). Risk management practices and financial performance of commercial banks in Kenya. *International Journal of Business and Public Management*, 2(1), 1–10.
- Mwangi, M., & Muturi, W. (2016). The effect of bank size on profitability of commercial banks in Kenya. *International Journal of Economics, Commerce and Management*, 4(11), 762–773.
- Mwega, F. M. (2016). Financial regulation in Kenya: Balancing inclusive growth with financial stability. In *Achieving Financial Stability and Growth in Africa* (pp. 233–262). Routledge.
- Mwithi, J. M. (2015). Strategies Adopted by Commercial Banks in Kenya to Combat Fraud: A Survey of Selected Commercial Banks in Kenya. *International Journal of Current Business and Social Sciences*, 1(3), 1-15.
- Naivasha, M. M. (2021). Influence of Strategic Management on Fraud Mitigation within Commercial Banks in Kenya: A Case Study of Kenya Commercial Bank.
- Nawawi, A., & Salin, A. S. A. P. (2018). Employee fraud and misconduct: empirical evidence from a telecommunication company. *Information & Computer Security*, 26(1), 129-144.
- Ndlovu, S., & Sibanda, G. (2021). Digital banking security measures and fraud prevention in Zimbabwe. *Journal of Digital Banking*, 10(3), 67-81.
- Ndung'u, N. (2017). Economic drivers of fraud in Kenya. *African Journal of Economic and Management Studies*, 8(2), 145–160. <https://doi.org/10.1108/AJEMS-02-2016-0012>
- Ngotho, M. R. (2023). Operational Risk Management Practices and Fraud in Commercial Banks in Kenya (Doctoral Dissertation, University of Nairobi).
- Ngugi, B. K., & Nyang'oro, O. (2017). Effect of financial innovations on financial deepening in Kenya. *International Journal of Business and Management Review*, 5(4), 16–32.
- Ngugi, R., & Karina, B. (2016). Corporate governance and fraud in Kenyan banks. *Journal of Financial Regulation and Compliance*, 24(2), 172–189. <https://doi.org/10.1108/JFRC-07-2015-0034>
- Nigerian Deposit Insurance Corporation. (2021). Report on Deposit Insurance and Bank Fraud. Abuja: NDIC.
- Njanja, W. L., & Maina, R. N. (2018). Ethical climate and employee fraud in Kenyan banks. *Journal of Business Ethics*, 147(4), 735–748. <https://doi.org/10.1007/s10551-016-3282-8>

- Njoroge, J. (2023). Forensic accounting and fraud prevention in Kenyan banks. *Kenya Journal of Forensic Accounting*, 5(2), 22-37.
- Njoroge, P., & Githinji, F. (2020). Cybersecurity in Kenyan Banks: Challenges and Strategies. *East African Journal of Banking & Finance*, 16(1), 88-107.
- Njuguna, P. K., Maingi, S., & Kiria, S. (2021). Recruitment and employee training and organisational resilience in Kenyan hotels. *African Journal of Hospitality, Tourism and Leisure*, 10(3), 999-1012.
- Noe, R. A. (2020). *Employee training and development*. McGraw-Hill.
- Nwachukwu, G., Oladepo, O., & Avickson, E. K. (2024). Quality Control in Financial Operations: Best Practices for Risk Mitigation and Compliance. *World Journal of Advanced Research and Reviews*, 24(1), 735-749.
- Obeng, S., Iyelolu, T. V., Akinsulire, A. A., & Idemudia, C. (2024). The Transformative Impact of Financial Technology (Fintech) On Regulatory Compliance in The Banking Sector. *World Journal of Advanced Research and Reviews*, 23(1), 2008-2018.
- Odeyemi, O., Ibeh, C. V., Mhlongo, N. Z., Asuzu, O. F., Awonuga, K. F., & Olatoye, F. O. (2024). Forensic accounting and fraud detection: a review of techniques in the digital age. *Finance & Accounting Research Journal*, 6(2), 202-214.
- Odhiambo, A. (2020). Fintech and the Evolution of Banking in Kenya. *Journal of Financial Innovation*, 6(1), 42-59.
- Ogola, J. (2015). The Effect of Corporate Governance on Occurrence of Fraud in Commercial Banks in Kenya.
- Oguejiofor, B. B., Omotosho, A., Abioye, K. M., Alabi, A., Oguntoyinbo, F. N., Daraojimba, A. I., & Daraojimba, C. (2023). A review on data-driven regulatory compliance in Nigeria. *International Journal of Applied Research in Social Sciences*, 5(8), 231-243.
- Oguya, J. A. (2024). Determinants of occupational fraud occurrence in manufacturing companies in Kenya: moderated by macroeconomic factors (Doctoral dissertation, Strathmore University).
- Okiro, K., & Aduda, J. (2015). Fraud detection and prevention in Kenyan banks. *Journal of Financial Crime*, 22(3), 321–335. <https://doi.org/10.1108/JFC-03-2014-0015>
- Okoro, P., & Adewale, T. (2023). Fintech solutions for fraud prevention in Nigerian banks. *Journal of Financial Technology*, 9(1), 15-27.

- Okoye, E. I., & Akamobi, N. L. (2009). The role of internal audit in fraud control in Nigerian banks. *Journal of Financial Crime*, 16(4), 370–386. <https://doi.org/10.1108/13590790910993708>
- Olaoye, G. O. (2024). Explainability And Interpretability in Fraud Detection Models.
- Olojede, P., Iyoha, F., Egbide, B.-C., & Erin, O. (2020). Regulatory agencies and creative accounting practices in Nigeria. *Problems and Perspectives in Management*, 18(3), 465-478.
- Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing The Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. *ACM Transactions on Management Information Systems (TMIS)*, 12(2), 1-29.
- Onyancha, V. A. (2023). Effect of Corporate Governance on Fraud Mitigation Among Microfinance Banks in Kenya. KCA University.
- Onyango, B. O. (2022). The Role of Fraud Management Policies in Mitigating the Severity and Reporting of Fraud Cases in the Public Sector: The Case of County Governments in Western Kenya (Doctoral dissertation, Strathmore University).
- Onyeama, J. (2024). Credit card fraud detection in the Nigerian financial sector: A comparison of unsupervised TensorFlow-based anomaly detection techniques, autoencoders and PCA algorithm. <https://arxiv.org/abs/2407.08758>
- Opiyo, L. A. (2023). Effectiveness Of Internal Control Systems on Fraud Detection and Prevention Among Small and Medium-Sized Enterprises in Nairobi Kenya (Doctoral Dissertation, Strathmore University).
- Osborne, J. W., & Waters, E. (2002). Four assumptions of multiple regression that researchers should always test. *Practical Assessment, Research, and Evaluation*, 8(2). <https://doi.org/10.7275/r222-hv23>
- Osei, S., & Boateng, D. (2021). Regulatory compliance challenges in Ghanaian financial institutions. *West African Financial Journal*, 17(4), 90-101.
- Otakefe, P. J., & Erujaroh, O. E. (2023). Mediating Effect of Chief Executive Officer Dominance on The Relationship Between Firm Attributes and Financial Fraud Likelihood. *African Development Finance Journal*, 5(2), 100-123.
- Otieno, P. O. (2021). Effects of ethical compliance on professional accountants in selected county governments of Kenya. University of Nairobi.
- Owino, E. O. (2019). The impact of regulatory compliance on performance of commercial banks in Kenya. *Journal of Finance and Accounting*, 3(1), 1–15.

- Owusu, G. M. Y., Koomson, T. A. A., Alipoe, S. A., & Kani, Y. A. (2022). Examining the predictors of fraud in state-owned enterprises: an application of the fraud triangle theory. *Journal of Money Laundering Control*, 25(2), 427-444.
- Oyelakin, O., & Abdullahi, A. (2022). Assessing the efficacy of employee training and internal control system on financial management of small and medium scale enterprises in Nigeria. *African Journal of Economic and Management Studies*, 13(3), 366-384.
- Palshikar, G. K. (2002). The Hidden Truth: A Case Study on Fraud Detection. *Information Systems Control Journal*, 2, 1-8.
- Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, 14(3), 01-16.
- Phiri, J., Lavhengwa, T., & Segooa, M. A. (2024). Online banking fraud detection: A comparative study of cases from South Africa and Spain. *South African Journal of Information Management*, 26(1), 1763.
- Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations and Society*, 38(6-7), 525–543. <https://doi.org/10.1016/j.aos.2012.07.004>
- Putra, I. M. Y. D., Rasmini, N. K., Gayatri, G., & Ratnadi, N. M. D. (2022). Organizational Culture as Moderating the Influence of Internal Control and Community Participation on Fraud Prevention in Village Fund Management During The COVID-19 Pandemic. *Linguistics And Culture Review*, 6(S1), 351-362.
- Rahman, N. H. A., Hamzah, N., Jamaluddin, A., & Aziz, K. A. (2019). Establishing an effective internal control system for fraud prevention: a structured literature review. *Asia-Pacific Management Accounting Journal*, 14(3), 21-47.
- Rai, A., & Acharya, N. (2021). The Impact of Technological Advancements on Fraud Detection in Financial Institutions. *Journal of Financial Technology*, 5(4), 112–130.
- Rai, T., & Acharya, K. (2021). Banking Frauds: Causes and Preventions. *Journal of Banking, Finance & Insurance*, 2, 70-85.
- Rashid, C. A. (2022). The role of internal control in fraud prevention and detection. *Journal of Global Economics and Business*, 3(8), 43-55.
- Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. R. (2022). An overview of corporate fraud and its prevention approach. *Australasian Accounting Business & Finance Journal*, 16(1), 101-118.

- Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. R. (2022). An Overview of Corporate Fraud and its Prevention Approach. *Australasian Accounting, Business and Finance Journal*, 16(1), 101-114.
- Razali, N. M., & Wah, Y. B. (2011). Power comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors, and Anderson-Darling tests. *Journal of Statistical Modeling and Analytics*, 2(1), 21–33.
- Reyns, B. W. (2025). Crime Pattern Theory, Rational Choice Theory, And Routine Activities Theory. *Understanding Crime Prevention*, 27-54.
- Riitho, V., & Wanjala, S. (2020). Impact of internal control systems on fraud detection and prevention in Kenyan Saccos. *Journal of Financial Regulation and Compliance*, 28(4), 530-545.
- Sawyer, L. B., Dittenhofer, M. A., & Scheiner, J. H. (2003). Sawyer's internal auditing: The practice of modern internal auditing (5th ed.). The Institute of Internal Auditors.
- Sharma, P., & Gupta, A. (2022). Blockchain-based fraud prevention methods in banking. *International Journal of Blockchain Applications*, 5(2), 52-67.
- Shwedeh, F., & Rwashdeh, B. (2023). The Moderation Effect of Artificial Intelligent Hackers on The Relationship Between Cyber Security Conducts and The Sustainability of Software Protection: A Comprehensive Review. *Migration Letters*, 20(S9), 1066-1072.
- Singh, A., & Laiboni, N. (2022). Comparative Analysis of Bank Fraud in Sub-Saharan Africa, *Journal of Financial Crime*, 29(1), pp. 304-322.
- Smith, I. H., & Kouchaki, M. (2021). Ethical learning: The workplace as a moral laboratory for character development. *Social Issues and Policy Review*, 15(1), 277-322.
- Smith, J., & Riley, T. (2019). Artificial intelligence in banking: The regulatory landscape and fraud prevention implications. *Journal of Financial Regulation*, 5(2), 210-230.
- Sofyani, H., Hasan, H. A., & Saleh, Z. (2022). The Moderating Role of IT Development on The Relationship Between Internal Control and The Quality Performance of Higher Education Institutions. *Quality Innovation Prosperity*, 26(2), 128-146.
- Soneji, P. T. (2022). The fraud theories: Triangle, diamond, pentagon. *International Journal of Accounting, Auditing and Performance Evaluation*, 18(1), 49-60.
- Soneji, P. T. (2022). The Fraud Theories: Triangle, Diamond, Pentagon. *International Journal of Accounting, Auditing and Performance Evaluation*, 18(1), 49-60.

- South African Reserve Bank. (2022). Guidelines on Cybersecurity for Financial Institutions. Pretoria: SARB.
- Ssekubwa, R. G. (2022). Money Laundering and Real Estate Sector in Kenya: Towards Robust Regulation (Doctoral Dissertation, Strathmore University).
- Sudirman, S., Sasmita, H., Krisnanto, B., & Muchsidin, F. F. (2021). Effectiveness Of Internal Audit in Supporting Internal Control and Prevention of Fraud. *Bongaya Journal of Research in Accounting (BJRA)*, 4(1), 8-15.
- Sukmadilaga, C., Winarningsih, S., Handayani, T., Herianti, E., & Ghani, E. K. (2022). Fraudulent Financial Reporting in Ministerial and Governmental Institutions in Indonesia: An Analysis Using Hexagon Theory. *Economies*, 10(4), 86.
- Supriadi, I. (2024). The Audit Revolution: Integrating Artificial Intelligence in Detecting Accounting Fraud. *Akuntansi Dan Teknologi Informasi*, 17(1), 48-61.
- Taber, K. S. (2018). The use of Cronbach's Alpha when developing and reporting research instruments in science education. *Research in Science Education*, 48(6), 1273–1296. <https://doi.org/10.1007/s11165-016-9602-2>
- Tan, J., & Wong, S. (2023). The use of artificial intelligence in fraud detection in banks. *AI and Financial Services Journal*, 14(2), 85-98.
- Thakur, V. (2024). Strategic Financial Management: Navigating The Banking Landscape. Dr Vishal Thakur.
- Trehan, M. A. (2024). An Impact Of Forensic Accounting Training On Strengthening Banking Fraud Controls. *Educational Administration: Theory And Practice*, 30 (1), 767-775.
- Tripermata, L., AK, S. A. S., Wahyudi, T., & Fuadah, L. L. (2021). The Driver of Whistleblowing Intention and Fraud Prevention: Attitude and The Ethical Culture of The Organization. *Sriwijaya International Journal of Dynamic Economics and Business*, 91-110.
- Utami, W., Nugroho, L., Mappanyuki, R., & Yelvionita, V. (2020). Early warning fraud determinants in the banking industry. *Asian Economic and Financial Review*, 10(6), 604-627.
- van Steenberg, E. F., & Ellemers, N. (2021). The social and organizational psychology of compliance: How organizational culture impacts on (un) ethical behavior.
- Vutumu, A., Aregbeyen, O., & Akinteye, A. S. (2024). Internal Control and Fraud Prevention in The Nigerian Public Sector: A Partial Least Square Structural Equation Modeling Approach. *Journal Of Financial Risk Management*, 13(4), 703-729.

- Wachira, M., & Ondigo, H. (2018). The effect of regional expansion strategies on the financial performance of commercial banks in Kenya. *International Journal of Finance and Accounting*, 3(1), 1–16.
- Wambua, J., & Mugambi, F. (2019). Commercial bank credit and economic growth in Kenya: An empirical analysis. *European Scientific Journal*, 15(13), 1857–7881.
- Wambura, J. C. (2023). The Influence of organizational culture and values in financial crimes prevention among technological multinational organizations in Kenya.
- Wanjohi, M. W. (2014). Fraud in the Banking Industry in Kenya: A Case of Commercial Bank of Africa.
- Waweru, N., & Kalani, V. (2019). Commercial banking crises in Kenya: Causes and remedies. *African Journal of Accounting, Auditing and Finance*, 6(1), 37–58.
- Waweru, N., & Mutua, J. (2022). Regulatory compliance and its effectiveness in reducing bank fraud in Kenya. *Journal of Kenyan Banking*, 19(1), 54-68.
- Were, M., & Wambua, J. (2014). Corporate governance and financial performance of commercial banks in Kenya. *African Journal of Economic and Management Studies*, 5(2), 128–143. <https://doi.org/10.1108/AJEMS-03-2013-0025>
- Weske, U., Boselie, P., Van Rensen, E. L., & Schneider, M. M. (2018). Using regulatory enforcement theory to explain compliance with quality and patient safety regulations: the case of internal audits. *BMC health services research*, 18, 1-6.
- Weske, U., Boselie, P., Van Rensen, E. L., & Schneider, M. M. (2018). Using regulatory enforcement theory to explain compliance with quality and patient safety regulations: the case of internal audits. *BMC health services research*, 18, 1-6.
- Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and digital banking trends. *Journal of Applied Finance and Banking*, 10(6), 15-56.
- Willis, J. W. (2007). Foundations of qualitative research: Interpretive and critical approaches. Sage Publications.
- Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *The CPA Journal*, 74(12), 38–42.
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *CPA Journal*, 74(12), 38–42.
- Wronka, C. (2022). Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*, 25(1), 79-94.

Wronka, C. (2022). Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*, 25(1), 79-94.

Yoganandham, G. Transformative Impact: The Role of Modern and Innovative Banking Technologies in Driving Global Economic Growth. *Tuijin Jishu/Journal of Propulsion Technology*, 45(1), 2024.

Zuberi, O., & Mzenzi, S. I. (2019). Analysis Of Employee and Management Fraud in Tanzania. *Journal Of Financial Crime*, 26(2), 412-431.



APPENDICES
APPENDIX I INTRODUCTION LETTER

Ole Sangale Rd, Madaraka Estate,
P.O Box 59857 00200, Nairobi, Kenya.
Cell: +254 703 414/6/7, Twitter: @SBSKenya
Email: info@sbs.ac.ke or visit www.sbs.strathmore.edu



18th March 2025

To Whom It May Concern,

RE: FACILITATION OF RESEARCH – ROBI, JOSEPH MAGIGE

This is to introduce Robi, Joseph Magige who is a Master of Commerce (MCOM) Student at Strathmore University Business School, admission number MCOM/169104. As part of our MCOM Programme, Joseph is expected to do applied research and undertake a project. This is in partial fulfilment of the requirements of the MCOM course. To this effect, Joseph would like to request appropriate data from your organization.

Joseph is undertaking a research paper on “**MODERATING EFFECT OF STAFF TRAINING ON DETERMINANTS OF FRAUDULENT PRACTICES AMONG EMPLOYEES IN KENYAN COMMERCIAL BANKS.**” The information obtained shall be treated confidentially and shall be used for academic purposes only.

Our MCOM Programme seeks to establish links with industry, and one of these ways is by directing our research to areas that would be of direct use to industry. We would be glad to share our findings with you after the research, and we trust that you will find them of great interest and of practical value to your organization.

We appreciate your support and shall be willing to provide any further information if required.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Njoki Kiagiri'.

Njoki Kiagiri
Manager – Graduate Programmes Strathmore University Business School.

Association of African
Business Schools



Strathmore Business School is a Proud member of:



APPENDIX II QUESTIONNAIRE

INTRODUCTION

Dear Sir/Madam,

You are invited to participate in this survey on the moderating effect of staff training on the relationship between determinants of fraudulent practices among employees in Kenyan commercial banks. The purpose of this study is to assess how internal control systems, regulatory compliance, organizational culture, and technological advancements influence fraud prevention.

Your responses will remain **confidential** and will be used for **academic purposes only**. Please answer all questions honestly. If you have any questions, feel free to seek clarification.

Thank you for your time and participation.

Instructions:

- Do not write your name to ensure confidentiality.
- Tick (✓) the most appropriate response.
- Use the provided scale:

1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree

SECTION 1: DEMOGRAPHIC INFORMATION

(Please tick (✓) the appropriate box or fill in the required information.)

Item	Response Options
1. Gender	<input type="checkbox"/> Male <input type="checkbox"/> Female
2. Age Group	<input type="checkbox"/> 18-25 <input type="checkbox"/> 26-35 <input type="checkbox"/> 36-45 <input type="checkbox"/> 46-55 <input type="checkbox"/> 56 and above
3. Highest Level of Education	<input type="checkbox"/> Diploma <input type="checkbox"/> Bachelor's Degree <input type="checkbox"/> Master's Degree <input type="checkbox"/> PhD <input type="checkbox"/> Other (Specify) _____
4. Job Position	<input type="checkbox"/> Risk Manager <input type="checkbox"/> Compliance Officer <input type="checkbox"/> Internal Auditor <input type="checkbox"/> Governance Manager <input type="checkbox"/> Other (Specify) _____
5. Employment Type	<input type="checkbox"/> Permanent <input type="checkbox"/> Contract <input type="checkbox"/> Temporary

6. Years of Experience in the Banking Sector Less than 1 year 1-3 years 4-7 years
 8-10 years More than 10 years
7. Bank Tier Tier 1 (Large Bank) Tier 2 (Medium Bank)
 Tier 3 (Small Bank)

SECTION 2

1. Internal Control Systems

Statement	1	2	3	4	5
1. The bank has a whistleblowing mechanism that helps in reporting fraudulent activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. The bank has effective internal control systems that prevent fraudulent activities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Regular risk assessments are conducted to identify fraud risks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. There are clear policies and procedures in place to mitigate fraud.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Employee roles and responsibilities are well defined to prevent unauthorized transactions.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. The internal audit department effectively monitors fraud risks and irregularities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Internal control measures are regularly reviewed and updated to address emerging fraud risks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Regulatory Compliance

Statement	1	2	3	4	5
1. The bank complies with all regulatory requirements related to fraud prevention.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Regulatory bodies conduct frequent audits and inspections to ensure compliance.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Employees are well trained on compliance policies related to fraud prevention.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 4. Regulatory penalties are a strong deterrent against fraudulent practices.
- 5. The bank collaborates with regulators to enhance fraud detection and reporting.
- 6. The bank promptly addresses audit recommendations from regulatory bodies.
- 7. Compliance officers actively monitor and enforce fraud prevention policies.

3. Organizational Culture

- | Statement | 1 | 2 | 3 | 4 | 5 |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1. Ethical behavior is encouraged and rewarded in our bank. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Management sets a good example in preventing fraudulent activities. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Employees are encouraged to report suspicious activities without fear of retaliation. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. There are clear consequences for employees involved in fraudulent practices. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. The bank promotes transparency and accountability in financial transactions. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. The bank has a zero-tolerance policy for fraudulent activities. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7. Employees regularly receive ethics training to reinforce an integrity-driven culture. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

4. Technological Advancements

- | Statement | 1 | 2 | 3 | 4 | 5 |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1. The bank uses advanced fraud detection technology to monitor transactions in real-time. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Cybersecurity measures are regularly updated to prevent fraud. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Artificial intelligence and data analytics are used to detect fraudulent activities. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

4. The online banking platform is secure against fraudulent activities.

5. Technology adoption has significantly reduced fraud in our bank.

6. The bank invests in continuous innovation to enhance fraud detection systems.

7. Employees are trained on emerging fraud-related cybersecurity threats.

5. Fraudulent Practices (Dependent Variable)

Section 1: General Awareness of Fraud

1. Have you ever witnessed or been aware of a fraud incident within the bank?
 - Yes
 - No
2. How frequently do you believe fraud incidents occur in your department?
 - Very frequently
 - Occasionally
 - Rarely
 - Never
3. In the past year, do you think fraud prevention measures (such as audits, checks, and balances) were effective in detecting fraud?
 - Very effective
 - Somewhat effective
 - Not effective
 - I am unsure

Section 2: Perceptions of Fraud

4. Do you think employees in your department are likely to report fraudulent behavior if observed?
 - Yes, employees will report
 - No, employees will not report
 - I am unsure
5. In your opinion, what is the biggest risk factor for fraud in the bank?
 - Weak internal controls
 - Lack of employee training
 - Ineffective supervision
 - Other (please specify) _____

Section 3: Training and Prevention

6. Do you feel adequately trained to identify and report fraudulent activities?
 - Yes

- No
- 7. How often do you receive training on fraud prevention and reporting mechanisms?
 - Regularly (e.g., quarterly)
 - Occasionally (e.g., annually)
 - Rarely
 - Never
- 8. Do you feel the bank's current fraud detection measures (e.g., monitoring systems, audits, etc.) are sufficient to prevent fraud?
 - Yes, very sufficient
 - No, there are gaps
 - I am unsure

Section 4: Specific Fraud Incidents

- 9. Have you observed any suspicious financial behavior in the past year that could indicate fraud?
 - Yes
 - No
 - I am unsure
- 10. What actions do you believe should be taken to improve fraud prevention in the bank?
 - Increase monitoring and audits
 - Provide more employee training
 - Improve internal controls
 - Other (please specify) _____

6. Staff Training (Moderator)

Statement	1	2	3	4	5
1. Employees receive regular training on fraud prevention and detection.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. The bank provides periodic workshops on regulatory compliance and ethics.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Staff members are trained to use fraud detection technology and tools.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Employees are well-equipped to recognize and report fraudulent activities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Training programs enhance employees' ability to adhere to internal control policies.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. Fraud prevention training is tailored to specific roles within the bank.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

7. Employees receive refresher courses on fraud prevention and compliance policies.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

THANK YOU



APPENDIX III: LIST OF COMMERCIAL BANKS

1. Equity Bank Kenya Limited, part of Equity Group
2. Stanbic Bank Kenya Ltd, part of Standard Bank Group
3. Co-operative Bank of Kenya Ltd
4. Citibank N.A. Kenya, part of Citigroup
5. NCBA Bank Kenya PLC, part of NCBA Group
6. KCB Bank Kenya Limited, part of KCB Group
7. Absa Bank Kenya PLC, part of Absa Group
8. United Bank for Africa Kenya Ltd, part of UBA Group
9. Diamond Trust Bank Kenya Ltd, part of Diamond Trust Bank Group
10. Bank of Baroda (Kenya) Ltd, part of Bank of Baroda Group
11. I&M Bank Ltd, part of I&M Bank Group
12. Bank of Africa Kenya Ltd, part of Bank of Africa Group
13. Standard Chartered Bank Kenya Ltd, part of Standard Chartered Group
14. SBM Bank Kenya Ltd, part of State Bank of Mauritius Group
15. African Banking Corporation Ltd (ABC Bank)
16. Development Bank of Kenya Ltd, state-owned
17. National Bank of Kenya Ltd, state-owned
18. Consolidated Bank of Kenya Ltd, state-owned
19. Access Bank (Kenya) PLC, part of Access Bank Group
20. Guaranty Trust Bank (Kenya) Ltd, part of GTCO Group
21. Bank of India, part of Bank of India Group
22. Paramount Bank Ltd
23. Premier Bank Kenya Ltd
24. Credit Bank PLC
25. Guardian Bank Ltd
26. Family Bank Ltd
27. Kingdom Bank Ltd
28. Middle East Bank (Kenya) Ltd
29. Victoria Commercial Bank PLC
30. Spire Bank Ltd

31. Gulf African Bank Ltd
32. M Oriental Bank Ltd
33. Sidian Bank Ltd, part of the Centum Group
34. Commercial International Bank Kenya Ltd (CIB), part of CIB Group
35. Habib Bank, part of Habib Bank Group
36. DIB Bank Kenya Ltd
37. Ecobank Kenya Ltd, part of Ecobank Group
38. DIB Bank Kenya Ltd



APPENDIX IV: ETHICAL REVIEW APPROVAL LETTER



26th March 2025

Mr Robi Joseph,
joseph.magige@strathmore.edu

Dear Mr Robi,

RE: Moderating Effect of Staff Training on Determinants of Fraudulent Practices Among Employees in Kenyan Commercial Banks

This is to inform you that SU-ISERC has reviewed and approved your above SU-masters proposal. Your application reference number is SU-ISERC2812/25. The approval period is from 26th March 2025 to 25th March 2026.

This approval is subject to compliance with the following requirements:

- i Only approved documents including (informed consents, study instruments, MTA) will be used.
- ii All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
- iii Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
- iv Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 72 hours.
- v Clearance for the export of biological specimens must be obtained from relevant institutions.
- vi Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
- vii Submission of an executive summary report within 90 days of completion of the study to SU-ISERC.






Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) <https://research-portal.nacosti.go.ke/> and obtain other clearances needed.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Ambrose Rachier".

Mr Ambrose Rachier,
Chairperson; SU-ISERC

APPENDIX VI: RESEARCH LICENSE

 REPUBLIC OF KENYA	 NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION.
Ref No: 803315	Date of Issue: 04/April/2025
RESEARCH LICENSE	
	
This is to Certify that Mr. JOSEPH MAGIGE ROBI of Strathmore University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: Moderating Effect of Staff Training on Determinants of Fraudulent Practices Among Employees in Kenyan Commercial Banks for the period ending 04/April/2026.	
License No: NACOSTLP/25/417819	
Applicant Identification Number: 803315	Director General:  NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION
	Verification QR Code
	
NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.	
See overleaf for conditions	