

BINDURA UNIVERSITY OF SCIENCE EDUCATION
FACULTY OF COMMERCE
DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES



**AN EVALUATION OF THE EFFECTIVENESS OF ANTI-FRAUD MEASURES IN
COMMERCIAL BANKS IN ZIMBABWE. A CASE STUDY OF COMMERCIAL BANKS
IN HARARE CBD**

BY

MBUNDURE BRIAN TANAKA

(B212986B)

***A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE BACHELOR OF COMMERCE HONOURS DEGREE IN
FINANCIAL INTELLIGENCE OF BINDURA UNIVERSITY OF SCIENCE EDUCATION.***

JUNE 2026

APPROVAL FORM

Title of dissertation: An Evaluation of the effectiveness of anti-fraud measures in financial institutions in Zimbabwe. A case study of Commercial Banks in Harare CBD.

1. To be completed by the student:

I certify that the dissertation meets the preparation guidelines as presented in the Faculty guide and instructions for preparing dissertations.

Signature_____  _____ Date_____ 3 August 2026 _____

(Signature of student) (Date)

2. To be completed by the Supervisor:

This dissertation is suitable for presentation to the faculty. It has been checked for conformity with the Faculty guideline.

Signature_____  _____ Date_____ 3 August 2026 _____

(Signature of supervisor) (Date)

3. To be completed by the Chairperson of the Department.

I certify, to the best of my knowledge, that the required procedures have been fulfilled and the preparation criteria have been met in this dissertation.

 _____
Signature_____ Date_____ 21/8/26 _____

(Signature of Chairperson) (Date)

RELEASE FORM

STUDENT NUMBER: B212986B

TITLE OF PROJECT: Evaluating the effectiveness of anti-fraud measures in financial institutions in Zimbabwe. A case study of Commercial Banks in Harare

DEGREE TITLE: Bachelor of Financial Intelligence Honours Degree.

Permission is hereby granted to Bindura University of Science Education library to produce copies of this dissertation for scholarly and research purposes only. The rights and neither the project nor extensive extracts from it may be printed or otherwise reproduced without the author's approval.

Signature _____  _____ Date _____ 3 August 2026 _____

(Author's signature)

DEDICATION

I dedicate this project to my beloved parents, whose endless love, sacrifices, encouragement and unwavering support have been the foundation of my success. Their hard work and belief in me have made it possible for me to reach this important milestone. I also dedicate this work to my twin brother, who has been by my side throughout this journey. Your support, companionship and shared experiences have made every challenge easier and every achievement more meaningful.

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to Almighty God for His grace, guidance, strength and protection throughout my academic journey. Without His blessings and unfailing support, this achievement would not have been possible.

I am sincerely grateful to my supervisor for the invaluable guidance, patience, constructive criticism and continuous support provided throughout the course of this research. His expertise and insightful feedback played a significant role in improving the quality of this dissertation.

My deepest appreciation also goes to my beloved family and friends, namely Davis Mapurazi, and Great Takavada, for their unwavering encouragement, prayers, love and support throughout my studies. Their belief in my abilities motivated me to persevere even during challenging times. Despite the economic hardships we faced, they continued to stand by me and provide both emotional and financial support, for which I am truly grateful.

I would also like to extend my sincere thanks to Bindura University of Science Education and the Department of Intelligence and Security Studies for equipping me with the knowledge, skills and academic foundation necessary to undertake this research. The support, guidance and learning opportunities provided by the institution greatly contributed to the successful completion of this study.

To everyone who contributed in one way or another to the success of this research, I am deeply thankful. Your support and encouragement will always be appreciated.

ABSTRACT

Fraud remains one of the major challenges facing the banking sector, particularly as technological advancements continue to create new opportunities for fraud. This study evaluated the effectiveness of anti-fraud measures in commercial banks in Harare, Zimbabwe. The objectives of the study were to identify the common types of fraud affecting commercial banks, examine the anti-fraud measures currently implemented, assess their effectiveness, determine the factors influencing that effectiveness, and propose strategies to strengthen fraud prevention and detection.

The study adopted a descriptive cross-sectional research design guided by a pragmatic research philosophy with a quantitative orientation. Primary data were collected using self-administered questionnaires distributed to employees involved in fraud prevention, compliance, internal auditing, risk management, fraud investigation and information technology security within selected commercial banks in Harare. A purposive sampling technique was used and 41 usable questionnaires were obtained for analysis. Quantitative data were analysed using descriptive statistics, while responses from open-ended questions were analysed thematically to support and explain the quantitative findings.

The findings revealed that identity theft, card fraud, cyber fraud, loan fraud and insider fraud were among the most common forms of fraud experienced by commercial banks. The results further showed that anti-fraud measures such as internal controls, employee training, fraud awareness programmes, data analytics, audits, whistleblowing mechanisms and transaction monitoring systems contribute to fraud prevention and detection. However, the effectiveness of these measures is constrained by factors such as rapidly evolving technology, inadequate employee awareness, limited financial resources, weak enforcement mechanisms and challenges associated with cyber-enabled fraud.

The study concluded that although commercial banks in Harare have implemented a range of anti-fraud measures, fraud incidents continue to occur and have generally increased over recent years. This suggests that existing measures require continuous improvement to keep pace with emerging fraud risks. The study recommends increased investment in advanced fraud detection technologies, regular employee training and awareness programmes, strengthened internal controls, enhanced

inter-bank collaboration and improved regulatory support to strengthen the effectiveness of anti-fraud measures within Zimbabwe's banking sector.

LIST OF ABBREVIATIONS

ACFE- Association of Certified Fraud Examiners

AI- Artificial Intelligence

AICPA- American Institute of Certified Public Accountants

AML- Anti-Money Laundering

API- Application Programming Interface

ATM- Automated Teller Machine

BEC- Business Email Compromise

BERA- British Educational Research Association

BSI- British Standards Institution

CAAT- Computer-Assisted Audit Techniques

CBD- Central Business District

CFT- Combating the Financing of Terrorism

DIM- Digital Investigation Managers

FATF- Financial Action Task Force

FBI- Federal Bureau of Investigation

FIU- Financial Intelligence Unit

ID- Identity Document

IRS- Internal Revenue Service

IT- Information Technology

KPMG- Klynveld Peat Marwick Goerdeler

MFA- Multi-Factor Authentication

ML- Machine Learning

NIST- National Institute of Standards and Technology

PwC- PricewaterhouseCoopers

RBZ- Reserve Bank of Zimbabwe

SEC- Securities and Exchange Commission

SOC- Security Operation Centre

SPSS- Statistical Package for the Social Sciences

UK- United Kingdom

USD- United States Dollar

TABLE OF CONTENTS

APPROVAL FORM	i
RELEASE FORM	ii
DEDICATION	iii
ACKNOWLEDGEMENT	iv
ABSTRACT	v
LIST OF ABBREVIATIONS	vii
CHAPTER I: INTRODUCTION	1
1.1 Introduction	1
1.2 Background of the Study	1
1.3 Statement of the Problem	2
1.4 Purpose of the Study	2
1.5 Research Questions	3
1.6 Significance of the Study	3
1.6.1 To Commercial Banks in Harare	3
1.6.2 To Stakeholders and Clients	3
1.6.3 To Regulators and Policymakers	4
1.6.4 To Academia and Future Researchers	4
1.6.5 To the Researcher	4
1.6.6 To the Wider Banking Sector	4
1.7 Assumptions	4
1.8 Delimitations of the Study	4
1.9 Limitations	5
1.10 Definition of Terms	5
1.10.1 Fraud	5
1.10.2 Fraud Detection	5
1.10.3 Fraud Prevention	5
1.10.4 Fraud Risk	5
1.10.5 Commercial Banks	6

1.11 Organization of the Study	6
1.12 Chapter Summary	6
CHAPTER II: LITERATURE REVIEW	8
2.1 Introduction	8
2.2 Conceptual Framework	8
2.2.1 Fraud	8
2.2.2 Types of Fraud	9
2.2.3 Types of Anti-Fraud Measures	10
2.2.4 Factors Affecting the Effectiveness of Anti-Fraud Measures	12
2.2.5 Conceptual Framework (Diagram)	14
2.3 Theoretical Framework	15
2.3.1 Fraud Triangle Theory	15
2.3.2 Fraud Diamond Theory	16
2.3.3 Fraud Deterrence Theory	17
2.3.4 Fraud Management Lifecycle Theory	18
2.4 Empirical Evidence	19
2.4.1 Empirical Evidence on Types of Fraud in Commercial Banks	19
2.4.2 Empirical Evidence on Anti-Fraud Measures Adopted by Banks	21
2.4.3 Empirical Evidence on the Effectiveness of Anti-Fraud Measures	22
2.4.4 Empirical Evidence on Factors Influencing Anti-Fraud Effectiveness	24
2.5 Gap Analysis	25
2.6 Chapter Summary	27
CHAPTER III: RESEARCH METHODOLOGY	29
3.1 Introduction	29
3.2 Research Philosophy	29
3.3 Research Design	30
3.4 Sources of Data	30
3.4.1 Primary Data	30

3.4.2 Secondary Data	31
3.5 Research Instruments	31
3.5.1 Self-Administered Questionnaires	31
3.6 Sampling Techniques	32
3.7 Population	32
3.8 Sample Size	33
3.9 Validity	33
3.10 Reliability	34
3.11 Data Collection Procedures	34
3.12 Data Presentation and Analysis Procedures	35
3.13 Ethical Considerations	36
3.14 Chapter Summary	36
 CHAPTER IV: DATA PRESENTATION, INTERPRETATION AND ANALYSIS	 38
4.1 Introduction	38
4.2 Response Rate	38
4.3 Demographic Characteristics of Respondents	38
4.4 Types of Fraud Encountered in Commercial Banks	40
4.4.1 Fraud Types Observed	40
4.4.2 Frequency of Fraud Incidents	42
4.4.3 Trend in Fraud Incidents Over the Past Three Years	43
4.4.4 Fraud Type Causing the Greatest Financial Loss	43
4.5 Anti-Fraud Measures Currently Implemented	44
4.5.1 Anti-Fraud Measures in Place	44
4.5.2 Frequency of Fraud Awareness Training	47
4.5.3 Whistleblowing Mechanism	47
4.6 Perceived Effectiveness of Anti-Fraud Measures	48
4.6.1 Effectiveness and Frequency of Use of Specific Measures	48
4.6.2 Overall Perceived Effectiveness	50
4.6.3 Contribution to Customer Trust and Regulatory Compliance	51

4.7 Factors Affecting the Effectiveness of Anti-Fraud Measures	52
4.7.1 Rating of Limiting Factors	52
4.7.2 Thematic Analysis of Open-Ended Responses on Challenges	54
4.8 Thematic Analysis of Recommendations and Additional Comments	56
4.8.1 Recommended Actions to Improve Fraud Prevention and Detection	56
4.8.2 Additional Comments	58
4.9 Discussion of Findings	59
4.9.1 Common Types of Fraud	59
4.9.2 Anti-Fraud Measures Implemented	60
4.9.3 Effectiveness of Anti-Fraud Measures	60
4.9.4 Theoretical Interpretation	61
4.9.5 Challenges and Strategies for Improvement	62
4.10 Chapter Summary	63
 CHAPTER V: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS	65
5.1 Introduction	64
5.2 Summary of the Study	64
5.3 Conclusions	66
5.3.1 Common Types of Fraud in Commercial Banks	66
5.3.2 Anti-Fraud Measures Implemented in Commercial Banks	66
5.3.3 Effectiveness of Anti-Fraud Measures	66
5.3.4 Factors Affecting the Effectiveness of Anti-Fraud Measures	67
5.3.5 Contribution of Anti-Fraud Measures to Banking Operations	67
5.4 Recommendations	67
5.4.1 Investing in Anti-Fraud Technology	67
5.4.2 Employee Training	68
5.4.3 Implementation of Strict Internal Controls	68
5.4.4 Creation of a Robust Ethical Culture	68
5.4.5 Improved Collaboration between Banks and Regulators	68
5.4.6 Better Regulatory Enforcement	68

5.4.7 Customer Awareness Programs	69
5.5 Areas for Further Research	69
5.6 Chapter Summary	70
REFERENCES	71
APPENDIX A	79

CHAPTER I

1.1 Introduction

Commercial banking fraud in Zimbabwe has turned into one of the serious challenges that pose a threat to the stability of the financial system and confidence in depositors. According to the Reserve Bank of Zimbabwe (RBZ, 2023), commercial banking fraud caused financial losses in 2022 that amounted to more than USD 35 million, as a result of insider embezzlement, illicit electronic transactions, ATM skimming, and credit card fraud. In particular, Harare as the financial capital of the country has experienced a lot of cases of fraud which revealed some serious shortcomings. Even despite the implementation of internal control procedures and compliance systems, traditional preventive methods still lack proactivity and proper integration with new banking technologies.

1.2 Background of the Study

Fraud is an international problem that leads to poor financial performance and economic instability. The Association of Certified Fraud Examiners (ACFE, 2022) approximates that corporations lose around 5% of their annual earnings from fraud worth trillions of dollars. Major cases of fraud include the Wells Fargo scandal in America and 1Malaysia Development Berhad in Malaysia.

Fraud continues to be a major challenge in Africa. According to the 2018 Global Economic Crime and Fraud Survey, 77% of firms in South Africa were exposed to fraud. In addition, the Bank of Central Bank of Kenya issued new currency notes in 2020 to curb money laundering practices (African Union, 2021). Several billions of dollars have been lost every year affecting financial institutions, customers, and stakeholders.

The situation in Zimbabwe has not been an exception. Liquidation of Trust Bank Corporation after abuse of depositor's funds in 2013 revealed how deep fraud has become in the local banking sector. Commercial banks in Zimbabwe have lost over \$35 million in 2022 through fraud practices including insider abuse, cybercrimes, and ATMs skimming (RBZ, 2023). Being the financial centre of the nation, Harare is particularly exposed to fraud due to the existence of frequent cases that compromise depositor confidence and the stability of the system. Although there have been efforts from the regulatory authority in enforcing regulations and introducing antifraud mechanisms, the problem lies in poor integration of technology, lack of staff screening and enforcement.

1.3 Statement of the Problem

Financial fraud constitutes one of the increasing threats affecting commercial banks in Harare, and this is due to low depositor confidence and the potential danger to the system's stability. Even though commercial banks in Harare have put in place different ways of combating this threat through measures like the establishment of internal controls, compliance framework, and use of computerized systems, the cases keep occurring, thus posing questions on the efficiency of these measures.

Most studies carried out on fraud in the country explain the types of fraud and how regulatory authorities are responding to them, while leaving aside the question of whether these approaches are effective or not. There are no studies that have investigated whether they reduce fraud incidences, the rate at which fraud cases are detected, improve control effectiveness and depositor confidence.

Thus, the current study intends to fill this gap through an assessment of anti-fraud strategies adopted in commercial banks in Harare in terms of their effectiveness.

1.4 Purpose of the Study

The purpose of this study is to assess the effectiveness of anti-fraud measures in commercial banks in Harare, Zimbabwe. Specifically, it seeks to:

- I. To identify common types of fraud affecting commercial banks.
- II. To examine the anti-fraud measures currently implemented.
- III. To evaluate the effectiveness of these measures in reducing fraud incidents, improving detection speed, and strengthening depositor confidence.
- IV. To identify challenges faced by commercial banks in Harare in implementing antifraud strategies.
- V. To recommend evidence based strategies for improving fraud prevention and detection.

1.5 Research Questions

- I. How effective are anti-fraud measures in commercial banks in Harare in preventing fraud incidents, strengthening depositor confidence and detecting fraud?
- II. What strategies can be developed to enhance anti-fraud measures in commercial banks in Harare?
- III. What are the types of fraud prevalent in financial institutions, particularly Commercial Banks in Harare?

1.6 Significance of the Study

1.6.1 To Commercial Banks in Harare

Offers industry-wide knowledge of the pros and cons of existing anti-fraud mechanisms, allowing organizations to build on their internal controls, digital surveillance, and employee screening to prevent fraud and safeguard their reputation.

1.6.2 To Stakeholders and Clients

Contributes to restoring depositor confidence by identifying effective strategies that safeguard client funds and improve customer trust.

1.6.3 To Regulators and Policymakers

Presents evidence-based suggestions for the Reserve Bank of Zimbabwe (RBZ) and Financial Intelligence Unit (FIU), which would be beneficial for building regulatory frameworks and enhancing compliance within the banking industry of Zimbabwe.

1.6.4 To Academia and Future Researchers

It fills a clear research gap by empirically evaluating the effectiveness of anti-fraud measures, providing a foundation for comparative studies and future scholarship.

1.6.5 To the Researcher

This research helps improve the researcher's knowledge of preventing financial crimes and complying with rules and regulations in banking. It aids in intellectual development and practical understanding of fraud in commercial banks and financial institutions in Zimbabwe.

1.6.6 To the Wider Banking Sector

Findings can be shared beyond Harare, promoting collaboration, knowledge exchange, and adoption of best practices across Zimbabwe and the region.

1.7 Assumptions

- I. Data collection techniques will produce reliable and accurate results.
- II. Respondents have adequate information on internal and anti-fraud practices that can help in getting useful information.
- III. Respondents will participate in the research activities.
- IV. Findings will give the viewpoints of those who deal directly with anti-fraud procedures, even though their results may not be statistically generalizable for all financial institutions in Zimbabwe.
- V. Anti-fraud practices are always put into practice in commercial banks in Harare.

1.8 Delimitations of the Study

This research covers commercial banks working in Harare only, and does not include rural banks, microfinance companies and building societies. The research only includes employees dealing with fraud prevention, compliance, auditing, and IT security, and does not track any long term trend of fraud.

1.9 Limitations

Generalizability of results to other settings such as rural areas or non-commercial banks may be impossible because of purposive sampling method used. Limitations of resources have led to limited sample size and self-reporting data is a possible source of bias even though triangulation will solve this problem.

1.10 Definition of Terms

1.10.1 Fraud

According to Association of Certified Fraud Examiners (2024), fraud entails deceit with the aim of obtaining an unfair or illegal advantage or making an individual suffer a loss. The term fraud can refer to acts such as theft, abuse, collusion, misappropriation, temptation, and coercion among others (Wells, 2014).

1.10.2 Fraud Detection

Fraud detection refers to systematic processes used by organizations to identify suspicious activities that may indicate fraudulent behaviour (Brown, 2021).

1.10.3 Fraud Prevention

Fraud prevention consists of measures and strategies implemented by organizations to mitigate the risk of fraudulent activities (Ogunode & Dada, 2022).

1.10.4 Fraud Risk

Fraud risk is the potential exposure of an organization to deceptive or dishonest actions resulting in financial losses, reputational damage, or legal consequences (Reuters, 2024).

1.10.5 Commercial Banks

Financial institutions authorized to operate in the country of Harare offering deposit, loaning, and payment facilities. These banks include CBZ Bank, Stanbic Bank Zimbabwe, Standard Chartered Bank Zimbabwe, FBC Bank, Steward Bank, ZB Bank, Ecobank Zimbabwe, Nedbank Zimbabwe, and BancABC.

1.11 Organization of the Study

- I. Chapter One – Introduction: Gives the background of the study, problem statement, research objectives, research questions, significance of the study, assumptions, delimitations, limitations, definitions of terms, and structure of the study.
- II. Chapter Two – Literature Review: Examines the concept of fraud, types of fraud, anti-fraud strategies, factors that affect the success of the strategy, theoretical perspectives, empirical studies and literature gap.
- III. Chapter Three – Research Methodology: Discusses the research design, tools, sampling method, population, sample size, methods of data collection, and methods of data presentation and analysis.
- IV. Chapter Four – Data Presentation, Analysis and Discussion: Presents data analysis, findings from the quantitative and qualitative analysis, and discusses the findings in respect of the research objectives.
- V. Chapter Five – Conclusion, Recommendations and Suggestions for Future Research.

1.12 Chapter Summary

The chapter provided an introduction to the research topic, emphasizing the constant risk of fraudulent acts in commercial banks in Harare regardless of the measures in place. It described the context of fraud in terms of global, regional and local perspective. The problem statement that was developed was concerned with doubts regarding the current measures put in place and the objectives which were concerned with identifying types of fraud, evaluating anti-fraud measures, identification of influencing factors and creation of strategies for enhancing the anti-fraud measure process. This chapter further discussed the research questions, the significance of the study to different groups of people, assumptions, delimitation involving commercial banks in Harare only,

limitations of the study especially regarding lack of accessibility of data and definition of important concepts of fraud, fraud detection and fraud prevention. The following chapter will be dedicated to reviewing the literature on fraud types and anti-fraud measures among others.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

Fraud in Harare Commercial Banks is becoming increasingly important for financial stability and security in the country. According to Reserve Bank of Zimbabwe (RBZ, 2023), the financial losses resulting from frauds amount to over USD 35 million in 2022 as a result of insider embezzlement, unauthorized transfers through electronic payments systems, fraud and ATM skimming. Being the financial center of the country, Harare has experienced the fraudulent activities unevenly. The chapter provides the review of literature on fraud and anti-fraud measures. The concepts, theories and practices regarding these phenomena and their impact on the effectiveness of anti-fraud measures in commercial banks in Harare will be discussed. Specifically, the definitions and typologies of fraud, anti-fraud measures and factors influencing their effectiveness will be provided. The theoretical frameworks to be reviewed include Fraud Triangle, Fraud Diamond, Fraud Deterrence Theory, Fraud Management Lifecycle Theory and the empirical research from global and local contexts will be considered. The goal of the chapter is to point out the gaps in the existing research and practices and the ways of improvements in order to set the stage for further research.

2.2 Conceptual Framework

2.2.1 Fraud

According to Wells (2024) and Albrecht (2019), fraud is the act of intentionally deceiving for personal gains through either misrepresentation, concealment, or exploitation of trust leading to the detriment of the individuals or organisations. Contrary to unintentional mistakes, fraud is intentional in nature. Fraudulent acts are committed due to various motives such as financial pressures and organisational needs (Wang, 2016). The effects of fraudulent acts go beyond the victims and affect the entire economic setting, increasing operating expenses and compromising the reputation of financial institutions (Button, 2014). In Zimbabwe, insider conspiracy and cyber-fraud have had devastating impacts (RBZ, 2022).

2.2.2 Types of fraud

- i) **Definition of Identity Theft:** Identity theft can be defined as a criminal activity where an individual's private and sensitive information is stolen without his knowledge (ACFE, 2020). Criminals or fraudsters obtain private or personal data such as IDs or banking details from individuals and use them to carry out illegal activities or create new accounts (Federal Trade Commission, 2020). Two types of identity theft are phishing and impersonation. Phishing is the fraudulent practice of sending emails or setting up websites to lure users into divulging private information like passwords and credit card numbers to create an urgent atmosphere (Jones, 2022; Hong, 2012). Impersonation is an act where fraudsters masquerade as some other person to access private or financial information.
- ii) **Card fraud through electronic means:** Card fraud through electronic means involves the usage of unapproved electronic cards or card details to commit fraud transactions without authorization from the cardholder (Irwin, 2018). This kind of fraud has become prevalent in Harare with the RBZ (2022) noting an increasing number of cases of electronic banking fraud in the city. There are two types of methods used in electronic card fraud namely; card skimming and card trapping. Card skimming involves the usage of electronic equipment to harvest card details including numbers and passwords (FBI, 2020). Card trapping is the process where equipment is used to trap a card in the ATM (FBI, 2020).

- iii) Embezzlement:** Is where one person misappropriates money or property that was put under his/her management (ACFE, 2020). In commercial banks of Harare, collusions by insiders are rampant, whereby those who have access misuse their position for their personal gains by stealing money or securities of companies through their positions. Some common ways include account manipulation, making unauthorized withdrawals, or using company credit cards (Bologna, 2018).
- iv) Accounting Fraud (Financial Statements):** Accounting fraud occurs through the distortion of financial statements so as to deceive investors by hiding losses and inflating performances (ACFE, 2020; Jenkins, 2020). In Harare, this act of fraud reduces confidence among investors and weakens regulation since distorted reporting does not aid informed decision-making.
- v) Tax Evasion:** it is a crime whereby an individual deliberately avoids payment of taxes which are due to the government by means of misrepresentations, misreporting and manipulation of the tax system (Internal Revenue Service [IRS], 2020). This is mainly done through misrepresentation, misreporting, and abuse of tax havens.
- vi) Ponzi Schemes:** This is an investment fraud scheme which pays out gains to early investors through the investments of new investors rather than through actual profit-making (SEC, 2020). These schemes depend upon recruiting new participants in order to keep paying out, and inevitably collapse when the recruiting stops.
- vii) Insurance Fraud:** It is the conscious act of misleading an insurance company in order to receive money that is not due (Coalition Against Insurance Fraud, 2020). It may be done by individuals, companies, and even insurance companies themselves (Derrig, 2002). Types of insurance fraud include false claims, accidents that are staged and inflated losses.

2.2.3 Types of Anti-Fraud Measures

- i) **Segregation of Duties:** One of the key elements of internal controls is the process of ensuring that errors of fraud are not committed, which means that there is no possibility that an error of fraud will be committed by any worker in his or her day-to-day work. This element of internal control includes sharing responsibilities amongst different people or departments, which helps limit manipulation. For instance, in a business entity, there should be a separation between the individual charged with keeping custody of the asset and the person who accounts for it. This is because the same person cannot control different aspects of a transaction.
- ii) **Job Rotation:** This includes transferring workers from one task to another at regular intervals to avoid giving too much power to any individual in relation to that particular task. In doing this, manipulation and exploitation of the process for personal benefit are minimized (Messmer, 2020). Job rotation is popularly practiced as a risk mitigation strategy in financial firms because it becomes difficult for the employees to hide any fraudulent behavior over long periods of time.
- iii) **Authorization Processes:** This involves having all the transactions authorized by people who have been officially assigned or authorized to do so (Ferraiolo, Kuhn and Gavrila, 2015). The main elements involved here are access control and authentication. Access control ensures that only those who have the authority get access to confidential data and prevents its misuse (Brothby, 2009; NIST, 2015). Authentication confirms the identity of the users through processes such as biometric techniques, passwords and tokens among others (Halliday, Badenhorst and Solms, 2012).
- iv) **Data Analytics:** This is fraud prevention that uses complex mathematical algorithms and machine learning to detect and stop any frauds (Rashid, Agrawal and Sharma, 2022). Companies can monitor the transaction, behaviour of the employees, and the abnormality of their actions (Chambers and Dhiraj, 2020). Using this method, banks can notice anything abnormal before it leads to losses.

- v) **Robust Hiring Practices:** Good recruitment practices minimize the possibility of having employees who may commit fraud. According to Wells and Rose (2016), background checks, verifying references, and integrity tests are some of the measures that should be put in place. Ramamoorti, Morrison, and Koletar (2020) assert that such practices constitute an organization's anti-fraud culture since the recruitment of reliable employees is the first step toward preventing fraud.
- vi) **Training and Employee Awareness:** These training programs make employees aware of the risks involved with fraud, ways of reporting fraud, and the need for internal controls. These training programs develop a culture of integrity and vigilance in the organization (Morrison, 2020). According to Albrecht et al. (2020), awareness programs enable employees to identify the types of fraud and their involvement in detecting such frauds.
- vii) **Regular Audits and Fraud Hotlines:** Internal auditing is the process of examining and analysing the accounts and activities of an organization to establish their accuracy, completeness, and compliance with relevant regulations (Aremo, Oder and Beasley, 2020). Internal auditing is concerned with internal control and compliance issues (Institute of Internal Auditors, 2020), whereas external audit gives independent assurance (International Auditing and Assurance Standards Board, 2020). The compliance audit is meant to guarantee that the required laws and standards are being followed (Ramsay, 2020). The fraud hotline allows employees and customers to anonymously report on any suspicious behavior (Aremo and Beasley, 2020).

2.2.4 Factors affecting the effectiveness of Anti-Fraud measures

- i) **Level of Technology and Security Systems:** Organizations with robust cybersecurity measures, surveillance mechanisms, and payment systems have more capability to spot and thwart fraudulent activity. Poor cybersecurity mechanisms enable criminals to easily carry out fraud since hackers can use loopholes in the system. Technology such as encryption,

biometric identification, and two-factor authentication help in reducing fraud in financial institutions and other businesses (Whitman and Mattord, 2021).

- ii) Employee Awareness and Training:** A trained employee will be in a better position to recognize any fraudulent activity. Phishing, identity theft, and cybercrimes have to be taught to workers so that the fight against fraud can be more effective. The absence of such training means that the organization can be vulnerable to fraud and cyber crimes (Krutikov and Graycar, 2018).
- iii) Strong Internal Controls:** Internal controls such as separation of duties, auditing, appropriate authorization and proper accounting records can minimize chances of fraud. Such controls will be able to detect any discrepancies before there is any loss. Internal controls are essential in both government and business entities (Arens, Elder and Beasy, 2020).
- iv) Legal and Regulatory Framework:** Having strong cyber laws, anti-corruption laws, and proper enforcement mechanisms enhances the ability to fight fraud. In situations where there is a strict government action in terms of punishing the fraudsters, people are dissuaded from committing such acts.
- v) Organizational Culture and Ethics:** The culture of a workplace which fosters honesty, transparency, and accountability will lead to low levels of fraud cases. Employees will be discouraged from fraudulent practices when there are rewards for ethical behaviour. Nevertheless, an organization which has a corrupt culture might inadvertently encourage fraudulent behaviours among employees.
- vi) Financial Resources:** Organizations that have enough money to spend can go ahead and purchase high quality software for security and train their employees. Limited funds have an effect on how well organizations can conduct anti-fraud and cybersecurity activities (Button and Gee, 2013).

2.2.5 Conceptual Framework

According to the review of literature, the proposed conceptual framework for this study indicates that the efficiency of the anti-fraud mechanisms in commercial banks of Harare will be affected by two kinds of variables. The independent variables consist of the anti-fraud mechanisms themselves such as segregation of duties, job rotation, authorization procedures, data analysis, effective recruiting practices, training and awareness of employees and regular audits with fraud hotlines. The moderating variables consist of the variables affecting efficiency, which are technology and security systems, employee awareness and training, internal control system, laws and regulations, corporate culture and ethics and financial resources. The dependent variable consists of the efficiency of the anti-fraud mechanisms, which can be defined through fraud detection rate, recovery rate, fraud incidence and depositor confidence rate.

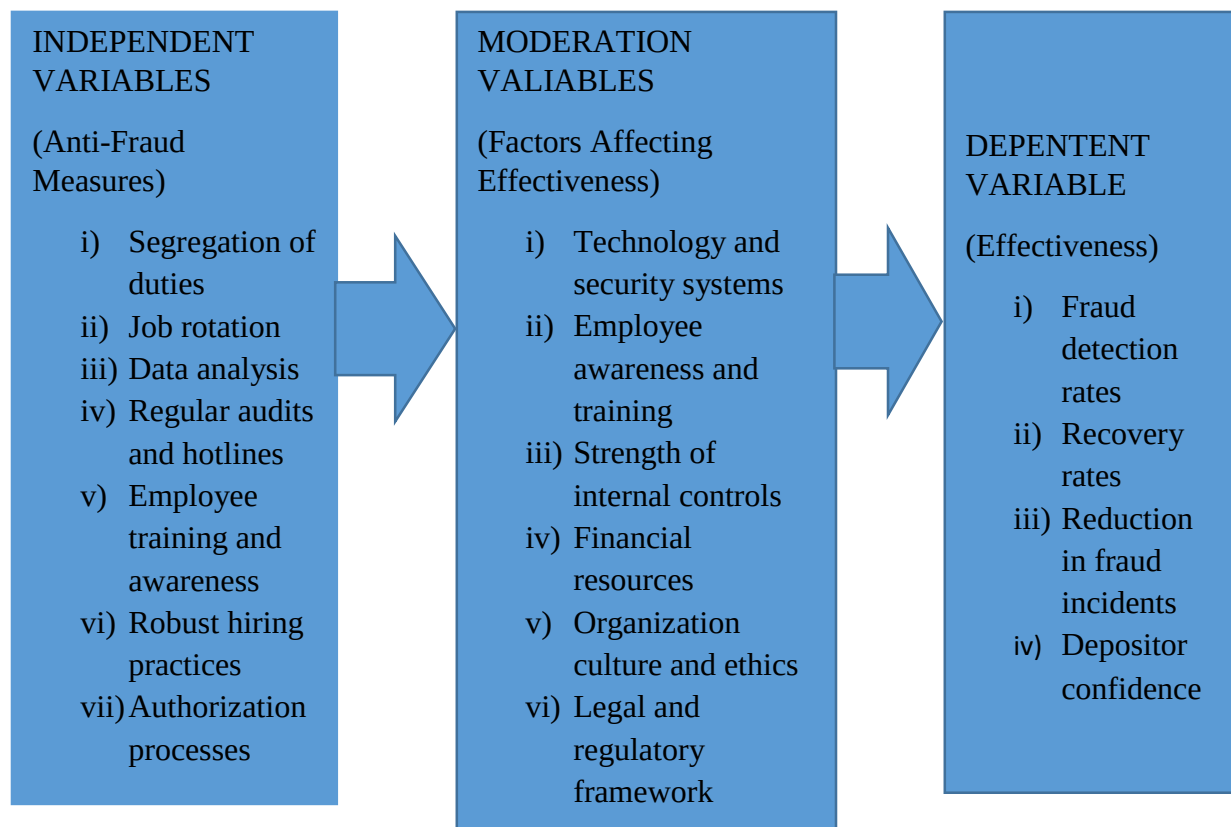


Figure 2.1: Conceptual framework showing the relationship between antifraud measures, moderating factors and effectiveness outcomes in Harare's commercial banks.

This model is used to guide the current study in showing that simply having fraud prevention strategies does not ensure their effectiveness. On the contrary, their effectiveness is dependent on certain environmental factors such as technology and culture. This will be done through empirical analysis of data gathered from commercial banks of Harare.

2.3 Theoretical Framework

2.3.1 Fraud Triangle Theory

Fraud Triangle theory is applied in understanding why people engage in financial misconduct and also to design controls aimed at preventing such behavior, which will be based on limiting the opportunities for fraud. The Fraud Triangle theory was invented by a criminologist known as Donald Cressey in the 1950s based on interviews with convicted embezzlers and was well documented in his work. According to Cressey, there are three basic elements, namely; pressure, opportunity and rationalization, which need to come together in order for one to commit financial fraud.

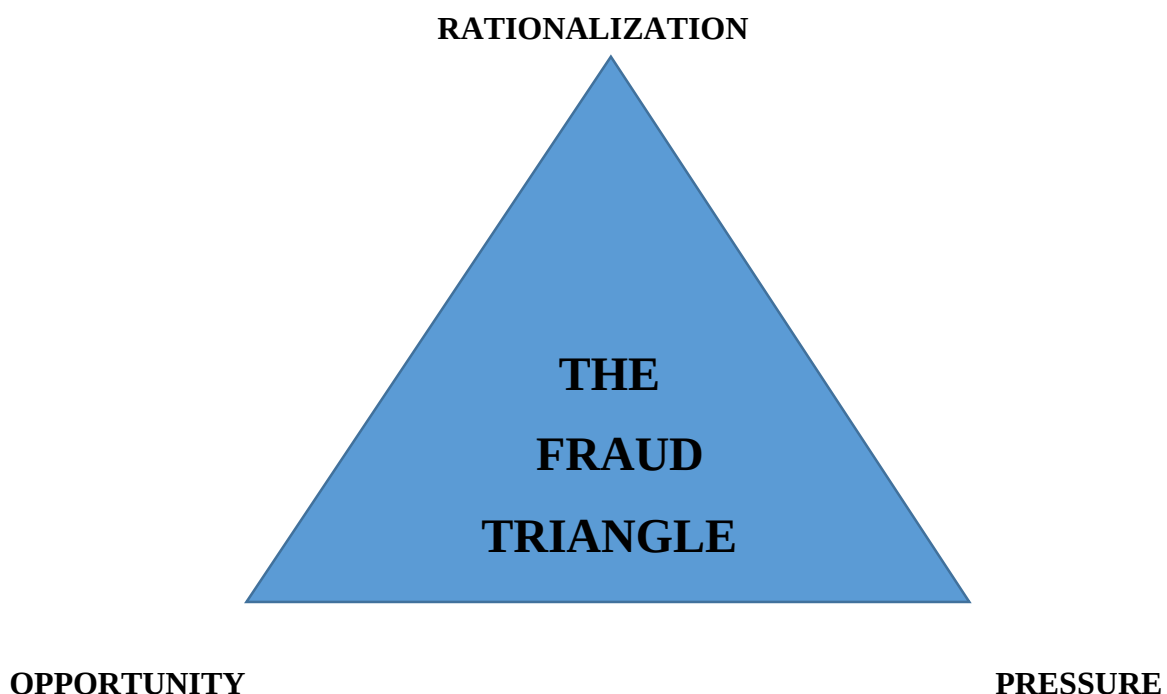


Figure 2.2: The Fraud Triangle Theory

- i) **Opportunity:** This happens when someone has an opportunity to commit fraud due to weak internal controls and being in a senior position within the organization to circumvent the system.
- ii) **Pressure:** This is usually a personal issue like being indebted, being a gambler, or the pressure to meet corporate financial goals which might be unrealistic.
- iii) **Rationalization:** This is an explanation made by the individual who has committed the act to feel okay about what they have done. Examples of rationalization are “I’ll pay it back,” “I’m underpaid,” and “Everyone does that.”

Relevance to the current study: The fraud triangle provides a model for evaluating anti-fraud measures on commercial banks in Harare by analysing whether existing controls reduce opportunity (segregation of duties), address pressure and counteract rationalization. This study will assess which elements of the triangle are mostly effectively managed and which remain vulnerable. For example, if a bank has strong technical controls but weak ethical culture, rationalization may remain a significant risk factor.

2.3.2 Fraud Diamond Theory

The Fraud Diamond Theory was conceptualized by David Wolfe and Dana Hermanson (2004). This theory builds on the Fraud Triangle theory by incorporating an additional fourth component. This theory states that fraud happens when there are four components existing together, which are pressure, opportunity, rationalization and capability (Wolfe & Hermanson, 2004).

- i) **Capability:** is the component that is added under the Fraud Diamond Theory. According to Wolfe & Hermanson (2004), in addition to pressure, opportunity and rationalization being key factors for committing fraud, the individual should be capable, competent and authoritative enough to do the same. For instance, a senior accountant who understands the financial system can commit and cover up the crime while a junior staff member cannot.

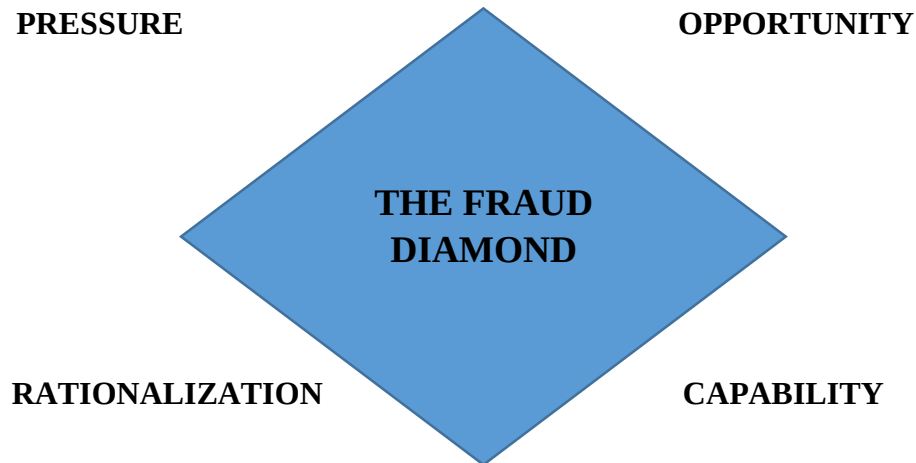


Figure 2.3: The Fraud Diamond Theory

Fraud Diamond Theory has been considered essential for fraud prevention since it assists organizations to detect weaknesses that motivate fraud through internal controls, audits, and ethics. Organizations can reduce chances of fraudulent acts by adopting this theory (Wolfe & Hermanson, 2004).

Relevance of the study: The inclusion of capability in the fraud diamond is especially important because of the commercial banks in Harare where electronic fraud demands a certain capability. This research paper aims to explore whether anti-fraud measures including access control and IT monitoring have taken care of the issue of capability or whether competent employees are still capable of circumventing all those mechanisms. According to this theory, even when pressure, opportunity, and rationalization are present, the fraud cannot be committed without capability.

2.3.3. Fraud Deterrence Theory

According to the Fraud Deterrence Theory, the chances of individuals conducting themselves fraudulently are minimized by the fear of detection and punishment. The theory suggests that the

potential fraudsters will consider the probability of getting caught and punished for the crime before carrying out the act. With severe and sure punishment, the potential perpetrators of the crime may not attempt fraud. The theory is connected to the writings of Cesare Beccaria (1764) and Jeremy Bentham (1789) that assert that well-enforced rules can minimize the chances of committing a crime including fraud. In organizations, the deterrence of fraud is achieved by implementing actions such as audits, internal controls, supervision, whistleblowing system and appropriate sanctions. According to Joseph T. Wells (2014), the employees will not commit fraud if they feel that their acts are under surveillance and the offenders are punished swiftly and appropriately.

Relevance to the current study: This theory plays an important role in evaluating the effectiveness of fraud prevention in commercial banks of Harare. When workers believe that it is difficult to detect fraudulent acts and there is no severe punishment for such acts, it becomes impossible to prevent the acts of fraud even when a great number of policies are available. In this research, it will be evaluated if Harare's commercial banks were able to create sufficient certainty of detection and severity of punishment that could help to prevent acts of fraud.

2.3.4 Fraud Management Lifecycle Theory

The Fraud Management Lifecycle Theory outlines the various stages that an organization goes through in its quest to prevent, detect, investigate and manage fraud. According to the theory, fraud management should not be seen as a one-off process. The theory was introduced by Wilhelm Hofmann (2008) who said that managing fraud requires a consistent approach.

Stages involved in the theory include deterrence, prevention, detection, mitigation, analysis, investigation, policy development and prosecution. In the case of deterrence, the goal is to deter people from committing fraud through proper control mechanisms, ethics and harsh punishment for fraud. When it comes to prevention, some of the measures that can be applied include staff training and having a secure financial system to reduce the likelihood of committing fraud. The detection stage is where audits, monitoring and whistleblowing are done to detect any fraudulent

activities. This is followed by investigations where organizations have to investigate the fraud case in order to find out who committed it.

As indicated by Hofmann (2008), the organizations that are able to manage all aspects of fraud management lifecycle successfully will be able to minimize financial loss as well as their reputation risk. It is significant for the theory since it makes organizations take a proactive approach towards managing fraud rather than just react to it.

Relevance to the current study: The Fraud Management Lifecycle Theory provides a process-based model for assessing the effectiveness of any measures against fraud. Instead of determining merely the existence of measures against fraud, the current study will determine whether Harare commercial banks cover all aspects of the cycle or only some of them (more attention to detection aspect of the cycle and less attention to other aspects such as deterrence and prosecution).

2.4 Empirical Evidence

2.4.1 Empirical Evidence on Types of Fraud in Commercial Banks

- i) Evidence of the various types of fraud in commercial banks in Zimbabwe is empirical as they include cases involving both conventional and technology-driven methods. Manhinde and Nkomo (2023) noted that fraud related to online banking such as phishing, card cloning, and vishing have escalated because of an increase in digital banking coupled with poor biometric controls. For instance, BancABC incurred losses of USD 1 million due to poor internal control in 2017 while Steward Bank lost USD 22 million due to vishing in 2021. In addition, Chitsora (2023) pointed out that embezzlement, document fraud, card fraud, and bribery are common cases of fraud in Zimbabwean banks. Collusion, bribery, and abuse of power was pointed out by Mabika (2015) in local governments in Zimbabwe, which is similar to the case of insider driven fraud in banks.

Critical analysis: Although all three articles tend to consistently point out electronic fraud and insider collusion as major types of fraud, their approaches diverge. The main focus of Manhinde and Nkomo (2023) is electronic fraud, whereas that of Mutambirwa et al. (2022) is traditional asset misappropriation. Such difference can indicate that the typology of bank fraud depends on the bank size, technological development, and regulation. Yet neither of the studies tends to measure the extent of financial losses caused by the specific type of fraud in Harare.

The Fraud Triangle (Cressey, 1953) describes the typologies in terms of pressure, opportunity, and rationalization. The Fraud Diamond (Wolfe & Hermanson, 2004) includes capability and the point that electronic fraud needs technical skills because the perpetrators take advantage of the weaknesses in information and communication technology. The collusion by insiders and the cyber fraud at commercial banks in Harare is an example of opportunity and capability.

- ii) On an international level, Capras and Achim (2024) conducted a study on corporate fraud in Romania during the period of 2010 to 2020 and determined that corporate fraud costs 5% of corporate income annually. These frauds include financial statement fraud (where revenues or assets are overstated while expenses and liabilities are understated), tax evasion, bankruptcy fraud, asset misappropriation and corruption. Although their work has focused more on Romania, the types of fraud mentioned in their study are applicable to the corporate world around the globe. However, the limitation associated with their study is that the regulatory and banking systems in Romania are different from those in Zimbabwe.
- iii) Reurink (2016) has defined the concept of financial fraud as one of the leading types of corporate fraud, providing categorization in terms of sources and means used for fraud. The author states that the financial fraud is a multifaceted problem that includes many types and motives such as financial statement fraud, financial scams (Ponzi scheme, pyramid scheme, advance-fee fraud, phishing scam), and fraudulent financial mis-selling. In contrast to studies conducted in Zimbabwe, Reurink (2016) is not based on empirical data but is conceptual in nature.

2.4.2 Empirical Evidence on Ant-Fraud Measures Adopted by Banks

- i) Anti-fraud measures adopted by commercial banks in Zimbabwe include traditional and contemporary techniques. According to Gwaka (2024) in a study on the use of fraud detection mechanism at ZB Bank Bindura, organizations adopt fraud detection mechanism and behavior-based early warning systems as required under RBZ regulations. Shungu and Mabuyaye (2024) showed that data analytics frameworks play a critical role in ensuring fraud detection and minimizing the number of cases by up to 86% using regression-based anomaly detection. Fraud detection and prevention efforts also involve forensic auditing as indicated by the findings of Mashayanye (2015) that forensic auditors detect fraud and identity theft but their success is limited by the lack of sufficient resources and managerial involvement.

Critical analysis: It is important to highlight the paradox that can be seen in the existing literature review. According to Gwaka (2024), the effectiveness of anti-fraud efforts was seen due to the fact that there was compliance with RBZ models. At the same time, Manhinde and Nkomo (2023) indicated that the detection rate of electronic fraud was 36%, while the recovery rate was 2%. It is evident that the paradox exists because of the distinction between perceived effectiveness and objective effectiveness of anti-fraud efforts.

The above approaches conform to the Fraud Management Lifecycle (Hofmann, 2008) that is characterized by prevention, detection, investigation, mitigation, and prosecution. The banks in Zimbabwe have implemented prevention, detection, and investigations in their fraud management framework, but deterrence and prosecution are still lacking.

- ii) On the international level, Mohammed, Asokan, and Arunasalam (2023) reveal the consequences of financial fraud committed in financial institutions, which have the knock-on effect of financial losses and instability in an economy. The number of institutions that experience fraudulent practices is more than 47% according to the results of the study. Anti-fraud measures mentioned in the research are digital forensic technologies that include artificial intelligence, computer assisted audit techniques (CAAT), security

operation center (SOC) and digital investigation manager (DIM). Their research reveals that 8% of the frauds are revealed through digital technologies. Other anti-fraud measures mentioned in the research are regulation including anti-corruption commission act, anti-money laundering act, personal data protection act and corporate policies. The limitation of the study is the Malaysian setting as compared to Zimbabwe.

2.4.3 Empirical Evidence on the Effectiveness of Anti-Fraud Measures

- i. As mentioned above, the findings from Gwaka (2024) indicated that the current fraud mitigation mechanisms are seen to be very effective due to their alignment with RBZ framework compliance. It is important to note that this is purely perceptual evidence since the current study, unlike Shungu and Mabuyaye (2024), did not provide empirical evidence of the effectivity of fraud mitigating measures in terms of 86 percent reduction of the number of fraud cases through regression-based anomaly detection.

It was established in the study conducted by Manhida and Nkomo (2023) that fraud detection rate and the recovery rate in case of electronic frauds were 36 percent and 2 percent respectively. It contradicts entirely the findings of Gwaka (2024) that the current anti-fraud measures are very effective. This contradiction will serve as the basis for further exploration of the current issue in Harare commercial banks.

Shungu and Mabuyaye (2024) empirically proved the two-way causality between data analytics and the decrease in fraud occurrence, proving that new technologies are better than traditional controls. The use of regression analysis makes their study more convincing compared to descriptive studies, however, since they used only one technological tool against fraud (data analytics), they have not provided any comparison of the effectiveness of anti-fraud measures.

According to the Fraud Deterrence Theory (Albrecht et al., 2006), there are two key components of deterrence: certainty and severity of punishment. In Zimbabwe, due to the

ineffective prosecution system and inability to recover losses, the probability of getting caught is too low, which does not provide any deterrence from committing frauds.

- ii. Flowerastia et al. (2021) revealed the fact that internal controls are highly important in fighting fraud, but awareness and corporate governance have little influence. Conducting the research using a quantitative approach, and collecting data via survey questionnaires among 100 participants working in start-up companies in Jakarta, Indonesia, Flowerastia et al. discovered the fact that internal control positively impacts the prevention and detection of fraud. It means that efficient internal control such as segregation of duties, reviews and access control is able to deter and detect the frauds. Nevertheless, their discovery that fraud awareness and corporate governance do not significantly influence fraud prevention does not match the conclusions of Albrecht et al. (2020). In particular, they stated that awareness is highly important for fraud prevention.
- iii. Mohammed et al. (2023) showed that the use of digital forensic tools and corporate policy has a positive correlation with reduced financial fraud in organizations. In a quantitative research study using survey data of the staff in financial institutions in Malaysia, they established positive correlations between digital forensic tools, regulation and corporate policy and reducing financial fraud. Therefore, these interventions are effective in fighting financial fraud. Nevertheless, the fact that the data was collected using self-reporting and is specific to Malaysia makes the results less generalizable to Zimbabwe.

Mutanda and Maireva (2023) revealed that cyber fraud prevention techniques are not entirely effective as fraudsters stay ahead technologically and the clients disregard the information in the awareness campaigns. Mandizvidza et al. (2020) revealed that forensic auditing is only effective if the auditors are properly trained although resource constraints affect its application. In summary, no single intervention can be used in fraud prevention but rather a combination of various approaches.

2.4.4 Empirical Evidence on Factors Influencing Anti-Fraud Effectiveness

- i) According to Manhida & Nkomo (2023), the inadequate use of machine learning and biometric technologies is another factor that contributes to electronic fraud. The research design adopted in this study is descriptive where questionnaires were used to gather data from a sample size of 100 respondents using both online and offline survey. The factors that affect effectiveness which have been established in the findings include; inadequate customer verification, ignorance of fraud frequency, non-cooperation of banks, poor legal representation in the criminal justice process, the difficulty of linking banking system and stakeholders' system, and failure to develop electronic registry for e-fraudsters. 75% of the participants felt that these factors made electronic banking systems vulnerable. One of the limitations of this study is that it is based on perceptual data alone.

- ii) As pointed out by Malle et al. (2021), organizational culture, internal control, commitment of the organization's leaders and allocation of resources were considered to be factors determining the level of success in the public sector of Tanzania. Through employing the mixed methods research design which involved the combination of both quantitative and qualitative data collection, it was established that among the respondents internal controls were the most successful strategy for prevention and detection of fraud followed by ethics and anti-fraud strategies. This study is not very relevant to the commercial banks in Zimbabwe.

- iii) According to Mabika (2015), the issues that act as barriers to combating corruption in local government in Zimbabwe include collusion, political interference, poor record keeping and shortage of resources. The research does not provide specific statistics; however, it provides an analysis from a qualitative perspective by conducting case studies and reviewing literature. The barriers listed above are ineffective segregation of duties, absence of supervision and monitoring, inadequate training and awareness program, collusion of internal personnel with outsiders, bribery, kickbacks, misuse of power and authority, financial problems, shortage of resources, understaffing, lack of expertise, political interference, poor implementation of anti-corruption regulations and inadequate

disciplinary actions among others. This is an extensive list of barriers. However, the study is restricted to local government rather than commercial banks.

- iv) According to Mutambirwa et al. (2022), there was poor quality of audit and lack of auditor independence which made fraud detection impossible in Zimbabwe's business environment. In this study, using a quantitative approach by administering questionnaires to 357 respondents from three cement manufacturing companies in Zimbabwe, the results indicated that internal auditing was unable to combat important types of fraud including check tampering, stealing money, misusing of corporate credit cards and improper payroll. This study indicated that although internal auditing is prevalent, its ability to detect fraud is limited. The limitation of this study is that the focus was on the cement manufacturing sector not banking.

2.5 Gap Analysis

Whereas there are a lot of studies that give useful information about fraud typology and anti-fraud mechanisms, there are few researches conducted on the performance of anti-fraud mechanisms in Harare's commercial banks. As an example, Manhida and Nkomo (2023) identified the increase in e-banking fraud, like phishing and card cloning, and also the study conducted by Mutambirwa et al. (2022), which addressed the fraud of payroll and check tampering. However, reports from FIU (2021) and RBZ (2022) show the persistence of the problem of fraud in commercial banks without any evaluation of their performance in practice. This research gives information about the typology of frauds but does not assess whether the existing mechanisms in Harare's banks reduce fraud incidents and help in recovering losses.

The specific gaps that have been identified in existing literature:

- i) Methodological gap: Local studies (Gwaka, 2024; Mutanda & Maireva, 2023) use perceptual data collected from questionnaires while not objective metrics such as fraud detection rates, recovery rates and fraud incidences are used.
- ii) Contextual gap: Research done in other countries (Capras & Achim, 2024 in Romania; Mohammed et al., 2023 in Malaysia) may not be applicable in the case of Zimbabwe

because of the uniqueness of its regulatory and economic environment, for instance, currency volatility, lack of technological capacity, among others.

- iii) Theoretical gap: Research done before does not test the efficacy of different fraud theories in predicting anti-fraud measures' success in Zimbabwean commercial banks. Such theories include Triangle, Diamond, Deterrence and Lifecycle.
- iv) Practical gap: There is no recent research that has analyzed detection rates, recovery rates and fraud incidences in several Harare-based commercial banks. Presently available studies consider one commercial bank (Gwaka, 2024 – ZB Bank Bindura) or one sector (Mutambirwa et al., 2022 – cement manufacturing).
- v) Temporal gap: Due to the constantly changing technological dynamics, including cyber crimes (Manhide & Nkomo, 2023), findings from studies that were conducted 10 years ago (Mashayanye, 2015) can no longer apply.

For instance, studies such as Mashayanye (2015) on forensic auditing and Shungu & Mabuyaye (2024) on data analytics indicate that there exist anti-fraud mechanisms but do not examine their effect in terms of reducing incidences of fraud, increasing speed of detection, or rebuilding depositor confidence in commercial banks in Harare. Furthermore, Gwaka (2024) gives some information on ZB Bank Bindura, although the findings at one institution cannot be used to generalize the findings for Harare commercial banks.

Many of the existing literatures concentrate on single institutions or generalize findings from other countries. They are useful but may not apply to the country's situation. Local literatures tend to focus on perception of risk of fraud rather than results (Mutanda & Maireva, 2023).

This study addresses the gaps identified above by:

- i. Assessment of the use and effective implementation of fraud measures in different commercial banks of Harare.
- ii. Using insights from employees, managers, and auditors through the use of quantitative and qualitative approaches such as questionnaires and interviews respectively.
- iii. Measurement of objective performance indicators like detection rates, recovery rates and trends of fraud.

- iv. Filling the gap between theory and practice by assessing how the different policies have been implemented.
- iv. Testing theories from Fraud Triangle, Fraud Diamond, Fraud Deterrence Theory, and Fraud Management Life Cycle.
- v. Offering contemporary and Harare-based data to the Zimbabwean financial industry.

The goal of this research is to assess the current effectiveness of anti-fraud measures, identify emerging challenges and propose innovative strategies tailored to Harare's commercial banking sector.

2.6 Chapter Summary

This chapter discussed both conceptual, theoretical and empirical literature on the subject of frauds and anti-fraud measures with emphasis on commercial banks in Harare, Zimbabwe. The conceptual definition of fraud included deliberate deception in an attempt to obtain some illegal gains with frauds being classified into identity theft, electronic card fraud, embezzlement and manipulation of financial statements among others. The measures to prevent frauds included both the conventional and contemporary methods of anti-fraud which involved internal control practices such as separation of duties and job rotation together with data analytics, forensic auditing and anti-fraud awareness campaigns. A conceptual framework indicating the relationship between the independent variables, moderating variables and the dependent variable was discussed.

The different theories covered in this chapter included the Fraud Triangle theory (Cressey, 1953), Fraud Diamond Theory (Wolfe & Hermanson, 2004), Fraud Deterrence Theory (Wells, 2014) and Fraud Management Lifecycle Theory (Hofmann, 2008).

Some empirical studies illustrated the strengths and weaknesses of measures. For instance, Shungu & Mabuyaye (2024) indicated the strength of data analytics in curbing fraud whereas Manhide & Nkomo (2023) uncovered weaknesses in electronic banking. Some reports of RBZ (2022) and FIU (2021) indicated huge amounts of frauds losses without evaluating the performance of anti-fraud

measures. Studies like that of Mashayanye (2015) and Gwaka (2024) focused on local institutions but findings were still scattered and descriptive in nature.

From the literature review, it is evident that there is a research gap in the topic. This is because there are many studies on fraud risks facing Zimbabwean banks but none evaluated the performance of anti-fraud controls in commercial banks of Harare. This gap necessitates this study because it intends to offer evidence-based recommendations.

CHAPTER III

RESEARCH METHODOLOGY

3.1 Introduction

This chapter focuses on the methodological approach used in the research in order to determine the efficacy of the measures designed to prevent fraud in commercial banks in Harare, Zimbabwe. This chapter starts with the discussion of the research philosophy and design, which are significant components to ensure the validity and reliability of the results obtained. Then, the methods of sampling that were used to obtain the sample from the target population will be discussed. The next section is devoted to the discussion of the data gathering techniques, including self-administered questionnaires used during the research and techniques of data analysis. Finally, ethical considerations will be discussed.

3.2 Research Philosophy

A pragmatist research philosophy with a prevailing positivist approach was used for this study. Pragmatism, according to Saunders et al. (2019), is applicable when the research question itself dictates the methodology choice and the researcher is not tied to one particular philosophic approach. The current study focused on effectiveness assessment and needed measurable and objective results, thus requiring comparison.

Positivism of the current study implies the existence of an objective reality with regards to incidents of fraud and implementation of anti-fraud measures regardless of personal views (Bryman, 2016). Creswell and Creswell (2018) state that positivism relies on quantitative research to collect the data using large sample sizes and make comparisons. Thus, the quantitative data collected with the help of questionnaires were used to establish trends in fraud cases and control

effectiveness. Even though open ended questions were included in the research design, the current approach can still be considered pragmatic as the focus is mainly on quantitative research. It provided answers to “what” (levels of effectiveness) but also helped to highlight the major challenges stated by respondents.

3.3 Research Design

Research design is the blueprint used to conduct research (Bryman, 2016). This particular study uses descriptive cross-sectional survey design. According to Neuman (2014), cross-sectional designs offer a snap-shot of what is currently being done within a specified time frame efficiently and effectively. The use of this design was appropriate considering that there was no need for any temporal tracking in this particular study.

This research can be described as being more quantitative as it uses a structured questionnaire with both closed ended and open ended items for collecting written comments. The use of these methods involves data summarization, data representation and analysis of closed ended items with consideration of the written qualitative comments (Creswell & Plano Clark, 2018).

3.4 Sources of Data

According to Zikmund, Babin, Carr and Griffin (2019), data is factual information that aids in reaching decisions. The sources of data for this study have been divided into primary and secondary data (Grafton Library, 2024).

3.4.1 Primary Data

Primary data are fresh data obtained especially for the purpose of conducting a specific study (Zikmund et al., 2019). As Saunders, Lewis & Thornhill (2019) put it, “primary data relate directly to the research questions”. In the current study, the researcher used self-administered questionnaires to collect primary data from employees of three commercial banks in Harare.

3.4.2 Secondary Data

Secondary data are those that have been gathered by others but not with the purpose of the ongoing research (Saunders et al., 2019). Such sources include academic journals, records from businesses, RBZ documents, FIU publications, and textbooks. As Bryman (2016) mentions, secondary data are an excellent base for research, as it allows establishing it within the context of existing knowledge. In the current study, secondary data was employed to provide some background information about fraud trends in the banking industry in Zimbabwe.

3.5 Research Instruments

The research instrument refers to any tool or method that can be used to collect, measure and analyse data (Creswell, 2018). Questionnaires served as the main instruments in this study since they were used in collecting primary data. The use of secondary data was used in ensuring.

3.5.1 Self-Administered Questionnaires

Questionnaires are known to be one of the major methods of collecting data (Neuman, 2014). The questionnaire comprises structured questions for obtaining data from respondents. As stated by Creswell and Creswell (2018), efficient questionnaires have to be clear, neutral, and should not contain complicated or leading questions. In the current study, both close-ended and open-ended questions were used in the questionnaire to receive more information. The questionnaire consisted of sections on demographic data, kinds of fraud faced, anti-fraud measures undertaken and their effectiveness. To get answers quickly, questionnaires were distributed face-to-face and online.

Advantages of questionnaires:

- Cost-effective and efficient for reaching a larger sample (Neuman, 2014).
- All participants received the same questions, ensuring consistency (Creswell and Creswell, 2018).
- Enabled rapid data collection over a short period.

- Increased respondent honesty and willingness to share sensitive information due to anonymity (Bryman, 2016).

Disadvantages of questionnaires and mitigation:

- Once administered, it is difficult to make changes to the questions. To address this, the researcher conducted a pilot test with five banking professionals before full distribution, following the recommendation of van Teijlingen and Hundley (2001).
- Questionnaires do not capture non-verbal cues such as body language or facial expressions.

3.6 Sampling Techniques

Sampling techniques describe the manner in which samples of populations are selected (Bryman, 2016). As stated by Leedy and Ormrod (2019), the main aim of the sampling process is to be able to obtain an accurate representation of the population features under certain allowable levels of error. In this particular research study, the sampling technique used is the purposive sampling technique.

According to Palinkas et al. (2015, p. 534), the purposive sampling technique is the selection of respondents using predetermined criterion that is related to the research aims. This technique was ideal for this research study since it needed participants who had specialized knowledge about anti-fraud measures (compliance officers, auditors, risk management, IT security). In the case of random sampling, there could be the chance of having staff who were not concerned with fraud. Purposive sampling cannot give generalizable results but gives rich information (Etikan, Musa & Alkassim, 2016).

3.7 Population

Population refers to the entire group from which the desired information is sought (Lind, Marchal and Wathen, 2017). Fraenkel, Wallen and Hyun (2012) indicate that in research, two categories of populations can be identified; target population (population in relation to which one wishes to

generalize the results of research) and accessible population (subset of the target population). In this case, the target population referred to all the employees working in the commercial banks in Harare and are responsible for fraud prevention, compliance, internal auditing, risk management and IT security. The Reserve Bank of Zimbabwe (2025) indicates that there are about 14 commercial banks in Harare with each having an average of 5-10 staff in these areas hence a total of 70-140 staffs. The accessible population was the employees of at least three commercial banks that allowed for the research.

3.8 Sample Size

In sampling, the sample is the selection of a small number of individuals within the target population who have similar qualities as the whole group (Bryman, 2016). Since it is impossible to conduct research on the whole population, it is necessary to choose a smaller number of individuals to represent the whole group (Saunders, Lewis & Thornhill, 2019). In this study, the sample consisted of 50 respondents for the questionnaire survey. According to Creswell (2018), for descriptive survey, a sample of 30-50 individuals is often adequate for descriptive statistics.

3.9 Validity

Validity is defined as how well a study measures what it wants to measure (Bryman, 2016). In the words of Trochim and Donnelly (2006), validity is what assures that research outcomes correctly reflect the phenomenon studied and are not affected by biases.

The questionnaire was tested in a pilot study and reviewed by the research supervisor for internal validity purposes. Haynes et al., (1995) define content validity as the coverage of items of an instrument for the measurement of a particular construct. The researcher sought feedback on the instrument from the research supervisor and conducted a pilot test on five bank personnel.

External validity (transferability) is reduced by purposeful sampling. However, Lincoln and Guba (1985) suggest that the provision of thick description of the context (commercial banks of Harare,

the regulatory environment, types of fraud) helps the reader judge whether the findings can be transferred to another setting.

3.10 Reliability

Reliability can be defined as the consistency and dependability of measurement tools and results (Field, 2018). In order for a study to be reliable, it must be replicable and it should yield the same results under the same conditions. According to Tavakol and Dennick (2011), one of the factors associated with reliability involves evaluating internal consistency of measurement tools, as it entails the assessment of the extent to which various questions yield similar results in measuring the same construct.

For the purpose of this study, the internal consistency of Likert-scale questions was evaluated with the use of Cronbach's alpha test. According to George & Mallery (2003), the alpha value greater than 0.7 signifies acceptable reliability. The value obtained was 0.78. It suggests that there was high internal consistency in the questionnaire items. The researcher kept a proper record of data collection and coding process.

3.11 Data Collection Procedures

Data collection was done for a period of eight weeks (weeks 3 to 10 from the timeline of the study) through the use of a questionnaire method as suggested by Creswell & Poth (2018). The procedures that were undertaken included

- i. Gaining permission: The researcher gained an introductory letter from Bindura University of Science Education and then made a request from the management of the participating banks. This conformed to the ethical access principles by Bryman (2016).
- ii. Piloting: The questionnaire was piloted among three banking professionals from a non-participating branch. According to van Teijlingen & Hundley (2001), piloting helps identify any ambiguous questions and practical issues. On the basis of feedback from pilot testing, two ambiguous questions were modified.

- iii. Questionnaire distribution: Questionnaires were distributed through two modes which included hard copies handed over personally to the bank premises and the online mode of sending a questionnaire link through email. Dillman, Smyth & Christian (2014) explain how mixed-mode distribution enhances response rates. A total of 50 questionnaires were distributed.
- iv. Questionnaire retrieval: Hard copies were collected after one week with a second reminder sent after two weeks. The response rate achieved was 82% (41 out of 50). Babbie (2016) explains that a response rate above 70% is very good in survey research.
- v. Documentation: Collection of relevant RBZ circulars, FIU annual reports and any anonymous bank fraud reports.

3.12 Data Presentation and Analysis Procedures

Data analysis began with detailed quality control measures to ensure the accuracy and completeness of the dataset including checks for missing values and outliers (Smith and Jones, 2023).

- i. Data Analysis for Quantitative Data: Data from closed ended questions in the questionnaires were coded and keyed in to Microsoft Excel and transferred to IBM SPSS (version 26). Descriptive statistics were conducted. Pallant (2020) suggests that descriptive statistics are suitable for summarizing survey data when describing patterns is the aim not testing any hypothesis. Findings were presented using tables, bar graphs, and pie charts.
- ii. Data Analysis for Open Ended Responses: Open-ended questions in the questionnaires received written answers, which were analyzed using thematic analysis according to Braun and Clarke (2006, p.87), which defined thematic analysis as a method of identification, analysis and interpretation of patterns within a set of textual data. Thematic analysis in this research was restricted to comments from respondents in the questionnaires. Recurring codes, such as weak enforcement, lack of training and insider collusion were identified as themes like regulatory challenges, capacity gaps and organization culture. These themes were used to support quantitative findings.

- iii. Integrating the findings: Integration of the quantitative findings with the themes from the open ended responses was done using narrative integration (Fetters, Curry and Creswell, 2013) in which qualitative comments illustrated or interpreted the patterns found in quantitative data.

3.13 Ethical Considerations

To guarantee the integrity of the research methodology, ethical considerations were prioritised. The study adhered to the ethical guidelines of Bindura University of Science Education and the principles outlined by the British Educational Research Association (BERA, 2018).

- i. Informed consent: All the participants got an information sheet on the purpose, procedures of the research, voluntariness of participation, and withdrawal right. Written consent was signed prior to the completion of questionnaires in accordance with the recommendations by Resnik (2015).
- ii. Confidentiality and anonymity: The names of the participants and banks were not included in the questionnaires. The data were saved on a password-protected laptop and available only to the researcher. Israel and Hay (2006) stress that confidentiality is of special importance when conducting research on sensitive areas, like fraud.
- iii. Minimisation of harm: No psychological and physical harm was expected to occur. Still, the researcher took into consideration possible repercussions in workplaces. The participants were assured that no individual responses would be disclosed to the employer based on the principle of beneficence (Beauchamp and Childress, 2013).
- iv. Permission: Permission was obtained from the Reserve Bank of Zimbabwe for sector-level data, as well as from the bank management of the participants. Ethical approval was acquired from the Faculty of Commerce of the university.
- v. Data storage: The raw data will be safely stored for three years after submission of the dissertation and then destroyed according to the data protection guidelines (BSI, 2019).

3.14 Chapter Summary

This chapter has provided an account of the methodology employed in assessing the success of fraud preventive measures in commercial banks in Harare, Zimbabwe. The chapter has described the pragmatic approach to research that is oriented towards the quantitative aspects of the research, the descriptive cross-sectional research design, as well as the use of self-administered questionnaires as the main instrument of collecting data. The purposive sampling technique has been applied to select 50 respondents who were asked to complete the questionnaires in three commercial banks. This chapter has covered issues related to data collection, data analysis, as well as validity and reliability.

CHAPTER IV

DATA PRESENTATION, INTERPRETATION AND ANALYSIS

4.1 Introduction

This chapter provides the analysis and interpretation of the findings generated by the self-administered questionnaire that was conducted among employees of three commercial banks in Harare, Zimbabwe, whose responsibilities include fraud control, compliance, internal auditing, risk management and IT security. The chapter starts by stating the response rate, followed by the demographics of the respondents. Then follows the presentation of the results regarding the nature of the fraud, anti-fraud measures currently in place, how effective these measures are and what is preventing them from being more effective. The responses to open-ended questions regarding the greatest causes of losses, biggest problems, measures needed and any other comment are then thematically analyzed using the approach of Braun and Clarke (2006).

4.2 Response Rate

In total, 50 surveys were handed out to compliance officers, internal auditors, risk managers, IT security experts, fraud investigators and chosen branch employees from three commercial banks in Harare. Out of these surveys, 41 surveys were received back as fully completed and usable, resulting in an 82% response rate. According to Babbie (2016), a response rate higher than 70% is considered excellent in survey research; hence the collected data could be considered to be representative enough of the opinions of fraud prevention staff from the sampled banks. All the percentages henceforth are calculated using $n=41$.

4.3 Demographic Characteristics of Respondents

Section A of the questionnaire consisted of the demographics of the respondents, which included gender, age category, highest level of qualification, job function, years of experience in the banking industry, and institution type. It is vital for determining the credibility of the respondents as sources

of informed opinions on anti-fraud practices since the study used purposive sampling of employees involved in the prevention and detection of fraud. Table 4.1 shows these demographics.

Table 4.1: Demographic Characteristics of Respondents (n = 41)

Variable	Category	Frequency	Percentage (%)
Gender	Male	19	46.3
	Female	18	43.9
	Non-binary	2	4.9
	Prefer not to say	2	4.9
Age group	20–29 years	12	29.3
	30–39 years	15	36.6
	40–49 years	12	29.3
	50+ years	2	4.9
Highest qualification	Diploma	4	9.8
	Bachelor's degree	19	46.3
	Master's degree	14	34.1
	Professional certification	2	4.9
	Other	2	4.9
Functional role	Risk management	11	26.8
	Internal audit	8	19.5
	Compliance	7	17.1
	IT security	7	17.1
	Fraud investigation / Financial Intelligence	5	12.2
	Other	3	7.3
Years of experience	Less than 2 years	6	14.6
	2–5 years	9	22.0
	6–10 years	18	43.9
	More than 10 years	8	19.5
Type of institution	Local commercial bank	22	53.7

Foreign-owned commercial bank	10	24.4
Building society	9	22.0

Regarding gender balance, the distribution is quite even in that males represented 46.3% of the respondents whereas females 43.9%, while a smaller percentage of 9.8% of the respondents did not identify themselves as male or female. As far as the age distribution of the respondents is concerned, the vast majority of respondents were aged between 20 and 49 years where the respondents within the age range of 30-39 years constituted the largest percentage (36.6%) in the distribution.

This implies that the respondents have been mostly sampled from a younger and cyber literate population which is significant for this research because of the increasing cases of fraud through cyberspace in this industry. On the aspect of qualification, the majority of the respondents had obtained a bachelor's degree (46.3%) and master's degree (34.1%) implying that the sample of respondents has been highly qualified to be able to give their views on fraud and its control mechanisms.

As far as the functional roles of the respondents are concerned, the most represented functions in the respondents' organizations included risk management (26.8%), internal audit (19.5%), compliance (17.1%) and IT Security (17.1%).

Most of the respondents (63.4%) had experience ranging from 6 to 10 years or more than 10 years in banking and financial institutions, indicating that the opinions that have been obtained are based on considerable institutional experience regarding the evolution of anti-fraud techniques. Last but not least, most of the respondents (53.7%) were obtained from local commercial banks while the rest were from foreign owned banks (24.4%) and building societies (22.0%).

4.4 Types of Fraud Encountered in Commercial Banks

This part of the paper will consider the first specific objective of this research, which was aimed at establishing the common forms of fraud that occur in commercial banks within Harare. The respondents were required to state the forms of fraud that have been occurring in their bank during the last 12 months, how frequent the occurrence of such cases is, the trend in the occurrence of

fraud cases in the last three years, and the form of fraud that has cost the bank the most money in the last three years.

4.4.1 Fraud Types Observed

Table 4.2: Types of Fraud Observed or Encountered (n = 41, multiple responses allowed)

Fraud Type	Frequency	Percentage (%)
Identity theft / impersonation	31	75.6
Card fraud (ATM skimming, cloning)	31	75.6
Cyber fraud (phishing, vishing)	28	68.3
Loan fraud (false documentation, misrepresentation)	27	65.9
Insider fraud / employee collusion	26	63.4
Cheque fraud	23	56.1
Money laundering through customer accounts	21	51.2
Financial statement fraud	16	39.0

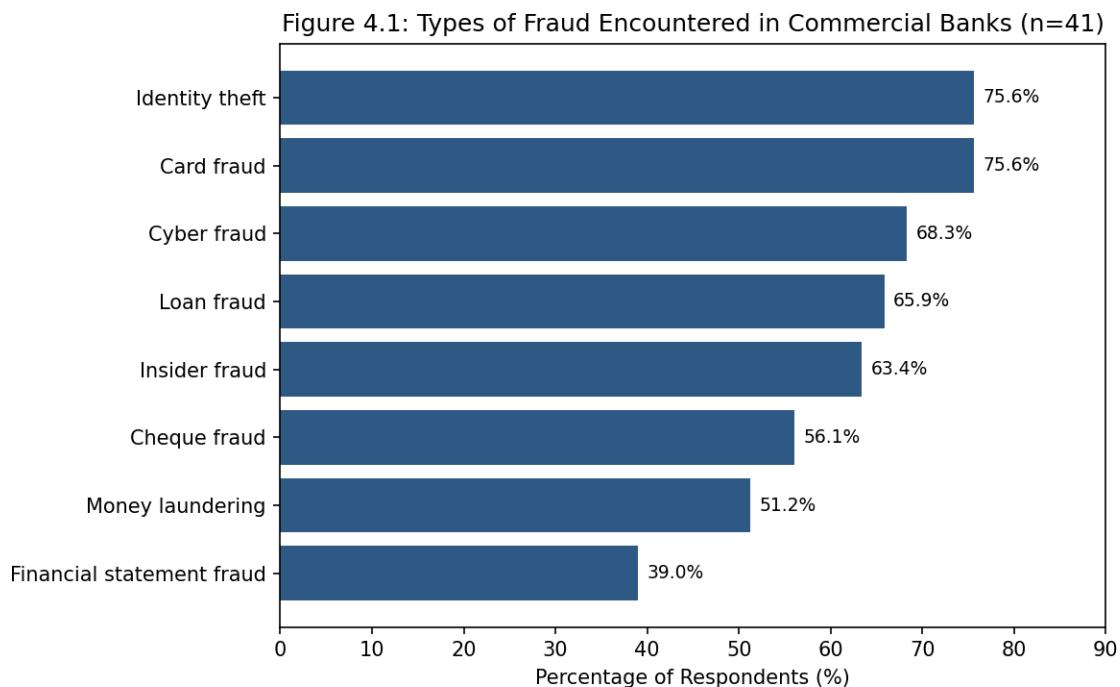


Figure 4.1: Types of Fraud Encountered in Commercial Banks (n = 41)

From the results, it is clear that identity theft/impersonation and card fraud such as ATM skimming and card cloning were the commonest type of frauds experienced by 75.6% of respondents. This is in line with Irwin (2018) and the RBZ (2022) who indicate that electronic card frauds have been on the rise in the banking industry in Harare. The cyber fraud type, which includes phishing, vishing, business email compromise (BEC), and API attacks, was confirmed by 68.3% of respondents.

The other common frauds include loan fraud (65.9%) and insider fraud/collusion (63.4%). This finding confirms that collusion fraud is the major form of fraud in the banking industry in Harare (Bologna, 2018; FIU, 2021). Other commonly reported frauds were cheques frauds (56.1%) and money laundering in customers' accounts (51.2%), while financial statements fraud was reported by only 39% of respondents. All in all, it is safe to say that there are numerous forms of fraud risks faced by commercial banks in Harare that cannot be easily put in any one basket. The above-listed forms of risk are not isolated but rather interconnected in terms of identity theft, credit card fraud, cybercrime, and even insider misuse.

4.4.2 Frequency of Fraud Incidents

Table 4.3: Frequency of Fraud Incidents

Frequency	Frequency (n)	Percentage (%)
Less than once per month	5	12.2
1–5 per month	14	34.1
6–10 per month	15	36.6
More than 10 per month	4	9.8
Unsure	3	7.3

On average, 46.4% said their respective banks have six or more fraud incidences per month; out of which, 36.6% have 6-10 fraud incidences while another 9.8% have over 10 fraud incidences per month. Only 12.2% had less than one incidence per month. It is clear from this data that fraud is

not a once in a while phenomenon but a daily challenge faced by anti-fraud officers in commercial banks of Harare. This is why the analysis carried out in this study has become so important.

In summary, the results indicate that instances of fraud take place quite frequently within commercial banks, underscoring the need to adopt anti-fraud strategies to reduce losses.

Figure 4.2: Further illustrates the frequency of fraud incidents in commercial banks, showing that the majority of respondents experienced fraud incidents between 6–10 times per month.

4.4.3 Trend in Fraud Incidents Over the Past Three Years

Table 4.4: Trend in Fraud Incidents Compared to Three Years Ago

Trend	Frequency (n)	Percentage (%)
Increased significantly	13	31.7
Increased slightly	14	34.1
Remained the same	7	17.1
Decreased slightly	7	17.1
Decreased significantly	0	0.0

However, the vast majority (65.8%) of those who participated in the survey reported that the number of occurrences of fraud had grown significantly (31.7%) and slightly (34.1%), while none reported a significant decline. These results are in agreement with the losses reported by RBZ (2023) to be over USD 35 million in 2022 and the 27% rise in the incidence of fraud cases using electronic banking facilities from 2020 through 2023 (RBZ, 2022). These results imply that the efforts taken to address fraud have been unsuccessful, and the level of fraud risk in Harare has increased instead of being reduced.

4.4.4 Fraud Type Causing the Greatest Financial Loss

In an open-ended question, participants were asked which fraud type has caused the most losses for their banks in the last three years. The responses have been thematically analyzed and grouped into different types of frauds, as shown in Table 4.5 below.

Table 4.5: Fraud Type Identified as Causing the Greatest Financial Loss.

Fraud Type	Frequency (n)	Percentage (%)
Cyber fraud (phishing, BEC, API/ransomware attacks)	13	31.7
Insider fraud / collusion	7	17.1
Card fraud / ATM skimming and cloning	6	14.6
Loan fraud	6	14.6
Identity theft / account takeover	3	7.3
Money laundering	3	7.3
Financial statement fraud	2	4.9
Cheque fraud	1	2.4

Cyber fraud, especially phishing, business email compromise, and API fraud, was reported to be the leading reason for financial losses (31.7%) and was followed by insider fraud or collusion (17.1%) and card fraud and loan fraud (14.6% each). Several participants underlined the irreversibility of cyber fraud losses and one participant highlighted that “Business email compromise against our suppliers and customers has caused the biggest financial losses, often leading to irreversible wire transfers,” and another participant pointed out that “Cyber fraud has been the most financially harmful, causing greater losses each year because of increasing criminal skills.” The participants who reported insider fraud as the costliest form of fraud highlighted the challenges in its early detection as “Insider fraud has been the most costly form of fraud due to the challenge of early detection and transaction values.” All these results support the conceptual framework in terms of capability and insider access as important factors determining the scale of fraud losses (Wolfe & Hermanson, 2004).

4.5 Anti-Fraud Measures Currently Implemented

This part focuses on the second research objective that aims at evaluating the anti-fraud strategies employed by commercial banks in Harare. The respondents were required to identify which of the fifteen anti-fraud strategies mentioned in the list have been put into use by their organization and the frequency of conducting formal training on fraud awareness.

4.5.1 Anti-Fraud Measures in Place

Table 4.6: Anti-Fraud Measures Currently Implemented (n = 41, multiple responses allowed)

Anti-Fraud Measure	Frequency	Percentage (%)
Segregation of duties	41	100.0
Formal authorization/approval processes	40	97.6
Regular internal audits focused on fraud risk	38	92.7
Mandatory fraud awareness training	35	85.4
Multi-factor authentication (MFA)	32	78.0
Customer transaction alerts	32	78.0
Cybersecurity awareness programs	30	73.2
Incident response plan for fraud	30	73.2
Robust hiring practices (background checks)	27	65.9
Whistleblowing hotline / confidential reporting	27	65.9
Job rotation for sensitive roles	24	58.5
Data analytics / automated fraud detection	24	58.5
Forensic auditing capabilities	23	56.1
AI / machine learning monitoring systems	22	53.7
Biometric verification	20	48.8

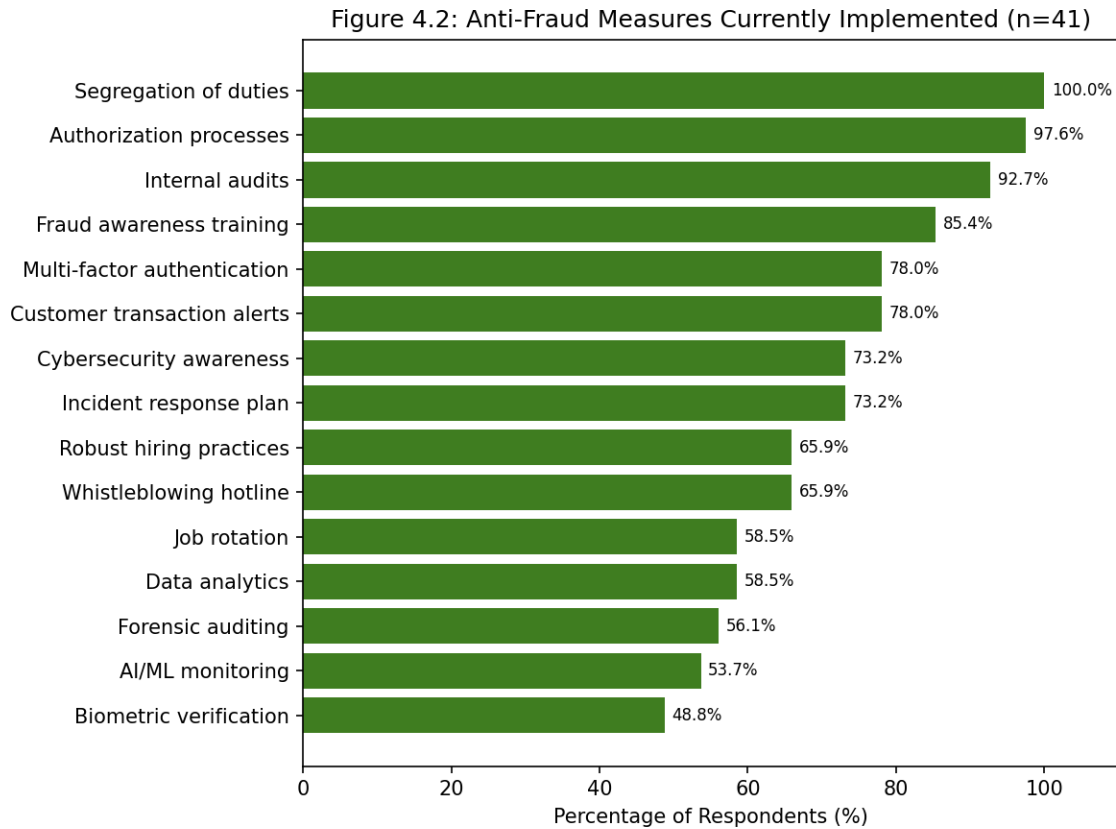


Figure 4.3: Anti-Fraud Measures Currently Implemented (n = 41)

Separation of duties was reported to be in use by all respondents (100%), while authorization and approval processes (97.6%) and internal audits (92.7%) were close to universal. The above results are in line with sound practices recommended by the Basel Committee (2018) and AICPA (2019) regarding internal control foundations including separation of duties, authorization controls and audits. Fraud awareness training was reported by 85.4% of the respondents, indicating the importance of training stressed by Albrecht et al. (2020).

In contrast, more sophisticated technology measures were adopted less universally. Multi-factor authentication (78.0%) and alerts for customer transactions (78.0%) were fairly common, but use of data analytics and automated fraud detection (58.5%), forensic auditing techniques (56.1%), AI machine learning monitoring systems (53.7%), and biometric verification (48.8%) was reported by more than half or fewer of the respondents. The above results are similar to observations of Munyanyi (2022) regarding low adoption of anti-fraud AI and block chain based technologies in African banks due to high costs and inadequate infrastructure, and KPMG Africa (2021)

conclusions about constrained adoption of more sophisticated controls in developing countries because of limited resources. The lower level of application of job rotation (58.5%) is also significant since according to Messmer (2020), it plays an essential role as a means of preventing any attempts of hiding fraudulent activities for a prolonged period and taking into account the fact that 63.4% of respondents mentioned.

4.5.2 Frequency of Fraud Awareness Training

Table 4.7: Frequency of Formal Fraud Awareness Training (n = 41)

Training Frequency	Frequency (n)	Percentage (%)
Never	2	4.9
Once a year	13	31.7
Twice a year	16	39.0
Quarterly	6	14.6
More than quarterly	4	9.8

Even though 85.4% of the surveyed people confirmed that they have been trained on fraud awareness (Table 4.6), Table 4.7 suggests that the rate at which this type of training is conducted is relatively low, since 36.6% of those surveyed receive the training once per year or not at all, whereas 39% receive it twice per year. Only 24.4% of the surveyed received training quarterly or more frequently. With the 65.8% of the surveyed confirming an increase in the number of fraud incidents over the last three years (Table 4.4), and the fast development of new methods used in cyber fraud, this low rate of training could hinder its effectiveness.

4.5.3 Whistleblowing Mechanism

Table 4.8: Existence and Use of Whistleblowing Mechanism (n = 41)

Status	Frequency (n)	Percentage (%)
Yes, and it is actively used	20	48.8

Yes, but it is rarely used	9	22.0
No	5	12.2
I don't know	7	17.1

While 65.9% of participants had already said that there was a whistleblowing line in existence (Table 4.6), Table 4.8 reveals that 48.8% of those interviewed were confident that this line was being utilized actively, while 22.0% admitted that the line was there but that it was not being used and 17.1% stated that they did not know if such a line existed or not. It is important to note that this gap in the existence and utilization of whistleblowing procedures is important in view of the Fraud Deterrence Theory (Wells, 2014) whereby it is not just the existence of the reporting mechanisms that matters but the perception that action will be taken without victimization.

4.6 Perceived Effectiveness of Anti-Fraud Measures

This chapter discusses the third research objective of the study, which is aimed at assessing the efficiency of the use of anti-fraud tools for the prevention and detection of fraud. The respondents were asked to indicate, on the five point scale (where 1 – not effective at all/never used, 5 – extremely effective/always used), both the efficiency of usage and the frequency of application of nine particular anti-fraud tools. Moreover, the overall efficiency of anti-fraud measures was assessed as well as their contribution to customer trust and regulation.

4.6.1 Effectiveness and Frequency of Use of Specific Measures

Table 4.9: Mean Perceived Effectiveness and Frequency of Use of Anti-Fraud Measures (n = 41, scale 1–5)

Anti-Fraud Measure	Mean Effectiveness	Mean Frequency of Use	Rank of (Effectiveness)
Segregation of duties	3.85	3.51	1

Whistleblowing hotline	3.85	3.51	1
Forensic auditing	3.80	3.51	3
Data analytics / automated monitoring	3.78	3.54	4
Background checks / robust hiring	3.76	3.46	5
Fraud awareness training	3.71	3.68	6
Job rotation	3.68	3.34	7
Authorization / approval processes	3.61	3.54	8
Internal audits	3.59	3.56	9

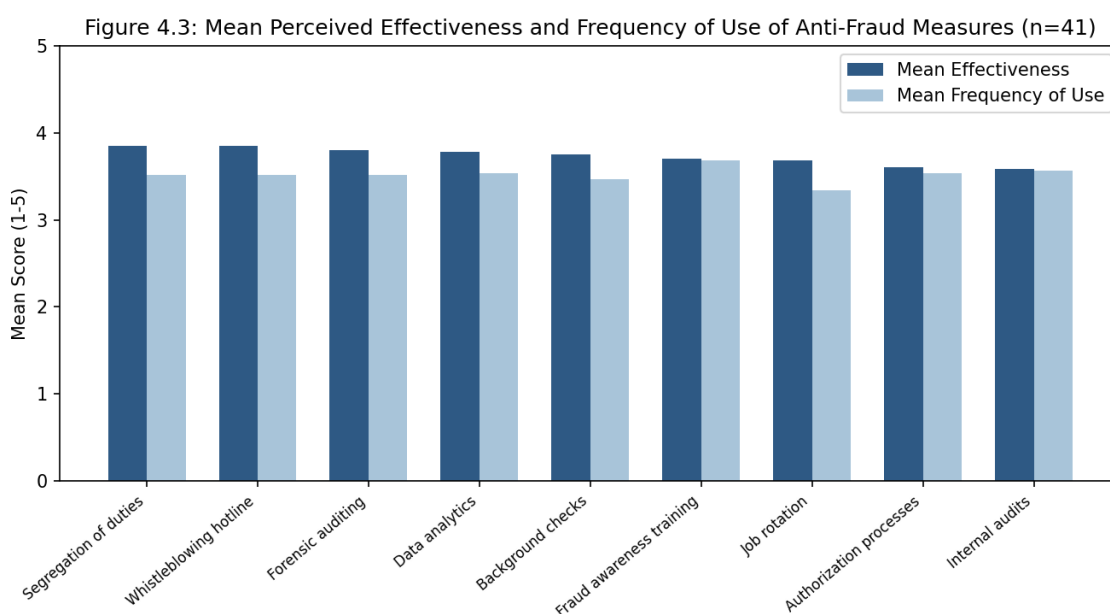


Figure 4.3: Mean Perceived Effectiveness and Frequency of Use of Anti-Fraud Measures

The mean effectiveness ratings for all nine measures fall within the range of 3.59 and 3.85 on the five-point scale, thus reflecting that while the measures in place are seen as effective enough, there is no single one measure that is seen as significantly better than the rest. The segregation of duties and the whistleblower hotline together emerged as the two most effective measures (with a mean rating of 3.85) followed by forensic audits (3.80) and automated monitoring (3.78). Interestingly, the internal audit process, which has close to 100% usage (92.7%, Table 4.6) emerges as the least effective control (with a mean rating of 3.59) along with the authorization/approval process (also with a mean rating of 3.61), implying that mere usage does not make controls effective, an

inference in agreement with that made by Okoye and Gbegi (2013) about the effectiveness of controls in Africa banks.

More importantly, the mean frequency of use of each measure was below its mean effectiveness score for all but one case. The largest difference occurred in the case of job rotation (3.34 compared to 3.68) and background check (3.46 compared to 3.76). In other words, certain measures, which are considered to be relatively effective, were not utilized as often as one would expect.

4.6.2 Overall Perceived Effectiveness

Table 4.10: Overall Perceived Effectiveness of Anti-Fraud Measures (n = 41)

Rating	Frequency (n)	Percentage (%)
Very ineffective	1	2.4
Somewhat ineffective	4	9.8
Neither effective nor ineffective	8	19.5
Somewhat effective	21	51.2
Very effective	7	17.1

Figure 4.5: Overall Perceived Effectiveness of Anti-Fraud Measures (n=41)

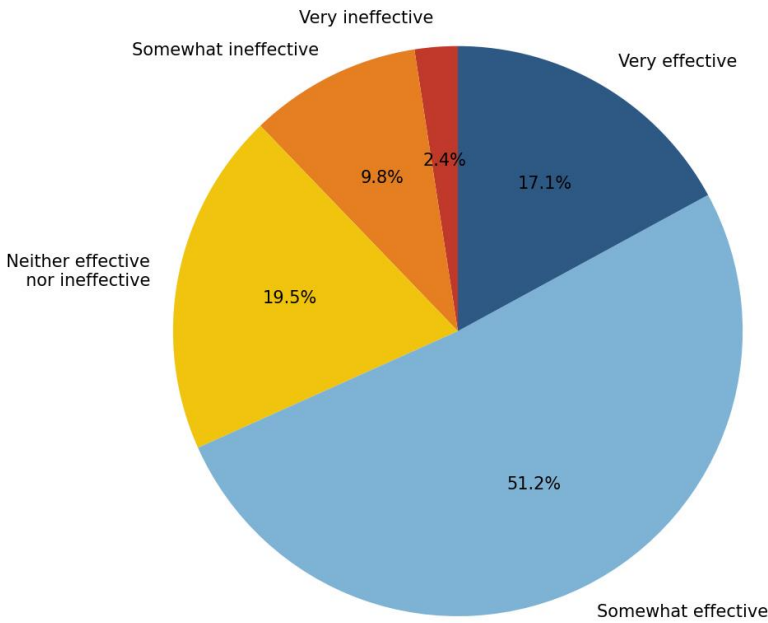


Figure 4.5: Overall Perceived Effectiveness of Anti-Fraud Measures (n = 41)

A total of 68.3% of participants felt that the currently implemented measures of preventing fraud at their respective banks were moderately effective (51.2%) or very effective (17.1%), indicating a mean of 3.71 (SD = 0.96) on the scale of effectiveness of these measures. On the other hand, 19.5% of participants were neutral about this issue, while 12.2% were either moderately or very ineffective with respect to this matter. This implies that while a clear majority of fraud prevention officers at Harare commercial banks feel that current measures are at least moderately effective in combating fraud, a significant number of people do not seem satisfied with the measures and find them insufficient, and very few respondents (17.1%) find the measures very effective indeed. Such results coincide with those reported by the FIU (2021) and RBZ (2022), indicating persisting fraud cases despite existing control measures, and prove the core assumption of the present research that the presence of anti-fraud measures does not ensure their effectiveness per se (Albrecht et al., 2016).

4.6.3 Contribution to Customer Trust and Regulatory Compliance

Table 4.11: Extent to Which Anti-Fraud Measures Contribute to Customer Trust (n = 41)

Extent	Frequency (n)	Percentage (%)
Not at all	1	2.4
Slightly	2	4.9
Moderately	5	12.2
Significantly	25	61.0
Don't know	8	19.5

Table 4.12: Extent to Which Anti-Fraud Measures Assist Regulatory Compliance (n = 41)

Extent	Frequency (n)	Percentage (%)
Not at all	1	2.4
Slightly	3	7.3
Moderately	8	19.5
Significantly	23	56.1
Don't know	6	14.6

Respondents agree that fraud prevention strategies not only prevent fraud but also serve as tools for developing customer trust (61%) and making banks compliant with various regulations, such as the RBZ regulations and AML/CFT standards (56%). The significance of this issue is determined by the fact that while some measures can be considered less effective by staff members in technical terms, the significance of their impact on the reputational and compliance-related factors remains significant. It fits into the general purpose of the research aimed at restoration of depositor trust and adherence to international standards, such as FATF (2020) and Basel Committee (2018). Still, it should be noted that a considerable number of employees stated that they were unsure whether there were links between the discussed measures and outcomes, such as customer trust (19.5%) and compliance (14.6%).

4.7 Factors Affecting the Effectiveness of Anti-Fraud Measures

This part will focus on the fourth objective of the research that aims at identifying the difficulties experienced by the commercial banks in Harare during the implementation of anti-fraud techniques. The participants were required to score eleven variables on a scale of one to five where (1) was for not a limitation and (5) was for a very severe limitation.

4.7.1 Rating of Limiting Factors

Table 4.13: Mean Ratings of Factors Limiting the Effectiveness of Anti-Fraud Measures (n = 41, scale 1–5)

Limiting Factor	Mean Score	Std. Deviation	Rank
Rapid technological change	3.95	1.16	1
Insider collusion across multiple departments	3.93	1.15	2
Organizational culture not prioritizing ethics	3.71	1.15	3
Sophistication of cybercriminals	3.66	1.13	4
Weak internal controls	3.54	1.14	5
Limited financial resources	3.49	1.33	6
Outdated or weak technology/security systems	3.27	1.00	7
Third-party / vendor vulnerabilities	3.22	1.39	8
Weak legal/regulatory enforcement	3.17	1.45	9
Limited AI / advanced detection capabilities	3.17	1.34	9
Inadequate employee training and awareness	3.02	1.19	11

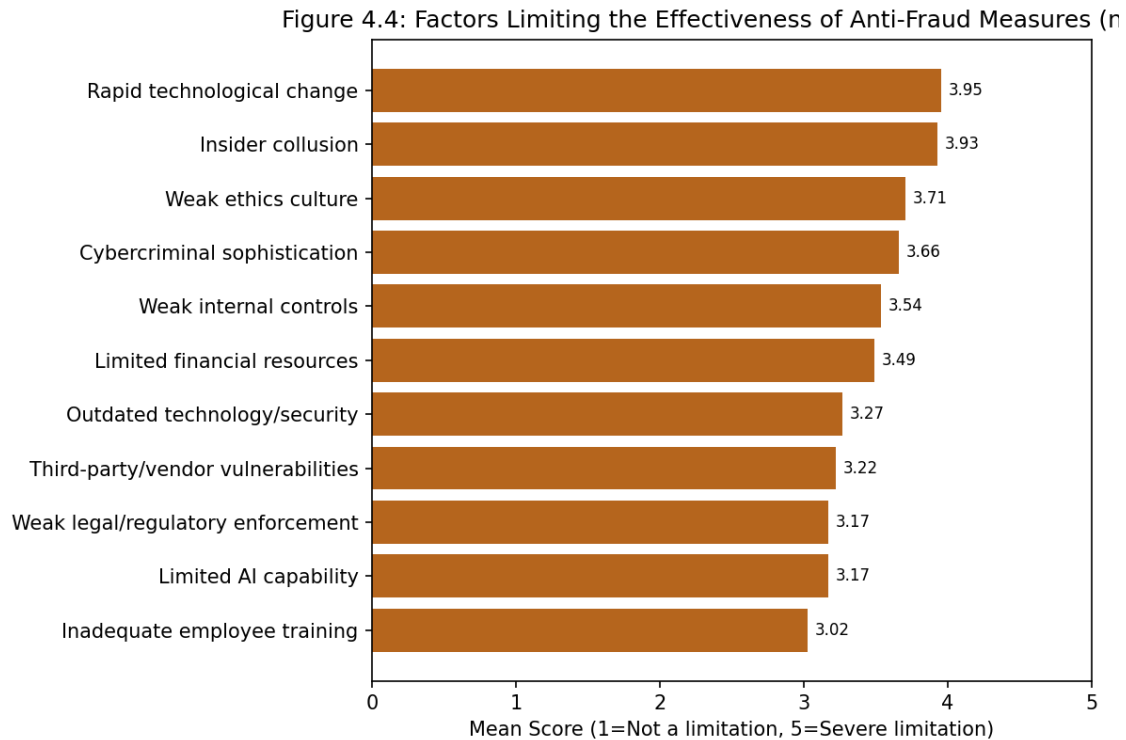


Figure 4.4: Factors Limiting the Effectiveness of Anti-Fraud Measures

The main limitation that respondents perceived to be a threat to the process of prevention of fraud was fast changing technology (average rating 3.95), while collusion among employees from different departments came second (3.93). The other two main limitations that emerged as a result were weak ethical climate in organization (3.71) and increasing sophistication of cybercriminals (3.66). It is worth mentioning that lack of employee training came last in the list (3.02), although training is rarely performed in any formal way.

This data is consistent with the theory developed earlier in this research paper. The high perception regarding the problem of collusion inside is particularly significant given that according to the Fraud Diamond Theory, people who have access to such information have a higher risk of fraud. At the same time, the high perception of technological changes and sophistication of cybercrime, together with the relatively low use of such advanced technologies as the use of AI or ML monitoring (53.7%) and forensic audit (56.1%) shows an alarming lack of ability of banks to deal

with the increasingly sophisticated fraud. The above idea corresponds to the statement made by Wells (2017).

4.7.2 Thematic Analysis of Open-Ended Responses on Challenges

Analysis of the open-ended questions regarding challenges or obstacles that hinder the effectiveness of fraud prevention was conducted in accordance with Braun and Clarke (2006), and six main themes emerged, as presented in Table 4.14 below.

Table 4.14: Themes Emerging from Open-Ended Responses on Challenges Limiting Effectiveness

Theme	Description	Illustrative Comment
Resource and technology constraints	Outdated systems, inadequate budgets for fraud detection technology, limited data analytics infrastructure, slow rollout of biometrics and legacy core banking systems incompatible with new fraud tools.	“The most significant challenge is the lack of adequate budget for modern fraud detection technologies. Many systems are outdated and unable to detect sophisticated cyber threats in real time.”
Human capacity and culture gaps	Insufficient frequency and depth of training, staff complacency, high turnover of compliance/investigation staff, and shortage of specialized digital forensics skills.	“Employee awareness remains a critical gap. Despite training programs, staff continue to fall victim to social engineering and phishing attacks.”
Organizational coordination weaknesses	Departmental silos between compliance, IT, operations and risk; inconsistent enforcement of controls across branches, unclear reporting responsibilities causing delays.	“Organizational silos prevent effective information sharing between fraud, compliance, IT security and risk departments, resulting in fragmented responses to fraud incidents.”

Insider threat and governance gaps	Controls designed primarily for external fraud, insufficient monitoring of privileged users, weak segregation of duties in smaller branches and gaps in pre-employment vetting.	“Insider threats pose the greatest challenge because existing controls were designed primarily to detect external fraud. Employees with system access can circumvent controls more easily than external attackers.”
External, regulatory and inter-bank gaps	Weak prosecution of offenders, absence of a centralized fraud intelligence database among Zimbabwean banks, and limited cross-border cooperation with regional financial intelligence units.	“There is no centralized fraud intelligence database shared among Zimbabwean banks, meaning known fraudsters can defraud multiple institutions without detection.”
Reporting culture and whistleblowing fears	Underutilization of whistleblowing channels due to fear of victimization, and management reluctance to escalate incidents due to reputational concerns.	“The whistleblowing mechanism is underutilized due to fear of victimization. Staff who witness fraud are reluctant to report it because of a perceived lack of confidentiality and retaliation risk.”

The findings in the open-ended responses support the results obtained in Table 4.13. The issue of resource constraints and out-of-date technology relates to the earlier identified problem that technological advancement is a key constraint and that there is moderate adoption of AI monitoring and data analytics technologies by banks. The insider threat theme explains why the problem of insider collusion received such a high rating (mean = 3.93). In a similar vein, concerns related to reporting culture and fear of whistleblowing account for the low use of existing whistleblowing hotlines despite their availability in most banks (65.9%) compared to their actual use (48.8%). The theme of gaps in the external and regulatory environment is supported by previous research in developing economies, which shows that the lack of effective law enforcement and inter-bank collaboration enables fraudsters to commit crimes with less risk. The findings are also consistent

with South Africa and Nigeria experience of the benefits of more robust auditing procedures, efficient whistleblowing, and fraud intelligence sharing. (Owolabi & Dada, 2013; PwC Africa, 2020).

4.8 Thematic Analysis of Recommendations and Additional Comments

The focus of this chapter is the fifth specific objective of the research, which was intended to establish ways that can help in the improvement of fraud prevention and detection. This chapter makes use of the suggestions made by the respondents, along with some other comments which have been put into categories based on the analysis done.

4.8.1 Recommended Actions to Improve Fraud Prevention and Detection

Table 4.15: Themes Emerging from Recommended Actions to Improve Fraud Prevention and Detection

Theme	Description	Illustrative Comment
Investment in technology and analytics	Real-time AI-powered transaction monitoring, behavior analytics, establishing baseline profiles, dedicated data analytics teams, cloud-based fraud detection platforms, zero-trust network architecture and regular penetration testing.	“Banks should invest heavily in AI-powered transaction monitoring systems that can detect anomalies in real time and trigger automatic alerts before fraudulent transactions are completed.”
Strengthening authentication and transaction controls	Mandatory multi-factor authentication for high-value/cross-border transactions, biometric verification and liveness detection at onboarding, automated alerts for dormant account reactivation and address changes, and transaction velocity controls.	“Multi-factor authentication should be mandatory for all high-value and cross-border transactions, with out-of-band verification to prevent interception.”

Training and capacity building	Mandatory quarterly, scenario-based fraud awareness training, customer education campaigns on social engineering, partnerships with universities to build a pipeline of fraud and forensic accounting specialists.	“A mandatory quarterly fraud awareness training programme should be implemented for all staff, using scenario-based learning drawn from actual fraud cases experienced by the bank.”
Governance, culture and accountability	Explicit “tone at the top” on zero tolerance for fraud, embedding fraud accountability into performance management, cross-functional fraud committees meeting monthly, and post-incident reviews feeding back into control design.	“Management should set an explicit tone at the top regarding zero tolerance for fraud, backed by consistent disciplinary action and prosecution of offenders regardless of seniority.”
Industry and regulatory collaboration	A centralized, RBZ-coordinated fraud intelligence database, a stronger RBZ supervisory framework assessing control adequacy, a peer-bank fraud response coalition, and lobbying for stronger whistleblower protection legislation.	“All banks should participate in a centralized fraud database coordinated by the Reserve Bank of Zimbabwe to flag known fraudsters and prevent them from operating across multiple institutions.”
Strengthening internal controls and process design	Strict, system-enforced segregation of duties, regular job rotation in sensitive departments, surprise fraud-focused audits, vendor cybersecurity due diligence, and embedding fraud risk assessment into product development.	“Segregation of duties should be strictly enforced across all branches and departments, with automated system controls that prevent a single user from initiating and approving transactions.”

4.8.2 Additional Comments

Further comments given by the respondents brought to light some of the problems identified in the research along with new issues. A large number of respondents believed the need for increased intervention at the national level and by the regulatory body. Respondents felt that RBZ needed to set out minimum standards for technology and procedure related to anti-fraud measures to be taken by commercial banks. The respondents also suggested the development of a central fraud reporting system and publication of anonymized statistics on fraud to benchmark the fraud level among different banks.

A few of the respondents mentioned new issues that had not been discussed much in the survey. These were the increasing use of artificial intelligence by fraudsters to create false identities and deep fake voices, use of cryptocurrencies for money laundering, and the use of mobile money services and instant payments system for fraud. These issues indicate the increasing sophistication and technological nature of fraud in the banking sector.

Another prevalent topic related to the importance of human and cultural components of fraud prevention. Some respondents pointed out that technical innovations alone are not enough if employees are not considering fraud prevention as one of their routine tasks. As one of the respondents said, the human factor is the weakest point still. Also, the problem of silence culture was mentioned by some respondents. They claimed that employees might be reluctant to report on the suspicious activity because of possible victimization and retaliation. Moreover, economic difficulties were seen as the cause of the insider fraud. According to some respondents, economic problems may push some people to commit fraud.

Inequity of resources in financial organizations was another issue which was discussed by some respondents. They argued that small local banks find it difficult to purchase advanced systems of fraud prevention in comparison to big banks or foreign financial institutions. In order to solve this problem, some participants suggested working together to overcome the problem.

In spite of all the worries, there have been some who admitted there has been improvement in fraud prevention policies in recent times. Increased commitment of management, increased awareness campaigns, and employee training have been recognized as positive steps. In addition to this, a few respondents even mentioned that an effective fraud prevention system can become a competitive advantage.

4.9 Discussion of Findings

This section synthesizes the findings presented above in relation to the study's research question, specific objectives, conceptual framework and theoretical frameworks discussed in Chapter Two.

4.9.1 Common Types of Fraud

The study also indicates that there are several types of fraud being experienced by banks in Harare. These include identity theft and card frauds, which are reported by three quarters (75.6%) of respondents each. Cyber fraud is also widely reported (68.3%). However, when respondents were asked what kind of fraud resulted in the largest losses, they indicated that it was cyber fraud (31.7%), followed by insider fraud (17.1%). It is worth mentioning an interesting contradiction – card fraud and identity theft occur much more often but they are usually small scale. On the contrary, cyber fraud and business email compromise as well as API-based fraud tend to cause bigger losses.

This information corresponds to the data provided in RBZ's report in 2022, where it was mentioned that the level of electronic banking fraud increased by 27% from 2020 to 2023, and also to the research done by Munyanyi (2022), who found out that cyber criminals tend to use banking systems more and more. Almost two thirds (65.8%) of respondents also indicated an increase in fraud incidents during the last three years.

4.9.2 Anti-Fraud Measures Implemented

As indicated in the results, the application rate of the basic low technological fraud control practices such as segregation of duties, authorizations and internal audits among banks in Harare is near 100% which conforms to the global best practices suggested by the Basel Committee (2018) and FATF (2020). The two international financial regulatory bodies agree that internal control should be the cornerstone for preventing any fraud in financial institutions. However, the rate of

advanced technological fraud control practices such as artificial intelligence monitoring (53.7%), forensic auditing (56.1%) and biometrics (48.8%) is only around 50%.

Such disparity between the adoption of basic control practices and advanced control practices can be explained by trends in African banking industry. According to the studies conducted by Munyanyi (2022) and KPMG Africa (2021), cost and technological infrastructure constraints usually slow down adoption of new technology. Such opinions have been echoed by the respondents from this research who identified budgetary constraints and old core banking systems as major barriers to adopting advanced fraud detection methods.

4.9.3 Effectiveness of Anti-Fraud Measures

In terms of the research questions, what level of effectiveness do the anti-fraud controls have in Harare's commercial banks? The data shows that it is moderate rather than high. All measures have been rated between 3.59 and 3.85 out of 5. Although almost two thirds of the participants (68.3%) consider the anti-fraud measures as somewhat and very effective, very few people (17.1%) see the measures as very effective, and there is also a noticeable percentage of respondents (12.2%) who believe that the measures are ineffective. This proves that although all necessary measures are present in commercial banks in terms of anti-fraud controls, the presence of such measures does not guarantee high effectiveness. In this case, it will be determined by other elements such as technology, training, regulation, culture and resources.

Surprisingly, the participants agree that the anti-fraud measures help to create customers' confidence (61%) and satisfy regulatory requirements (56.1%). Thus, even though the technical effectiveness is moderate, such measures have a great importance in terms of reputation and governance.

4.9.4 Theoretical Interpretation

The results of the present research study can be interpreted from the perspectives outlined in Chapter Two. Through application of the Fraud Triangle Theory (Cressey, 1953), it can be seen that there is much effort being made by the commercial banks in Harare to minimize opportunities for fraud through the implementation of segregation of duties and authorization. Nonetheless, the findings also showed weaknesses in other aspects of the theory. The high score given to organization's culture lacking ethical values (M=3.71) along with worries raised by the respondents regarding organizational culture of silence and influence of financial pressures on the employees indicates that the pressure and rationalization aspects of fraud are still insufficiently controlled. It seems that even though there is a control mechanism, the underlying issues are still creating vulnerabilities.

The results of the research can also be interpreted from the point of view of the Fraud Diamond Theory (Wolfe & Hermanson, 2004). One of the main factors preventing fraud from being efficiently controlled, as indicated by the respondents, was insider collusion (M=3.93). On the other hand, the relatively conservative application of technologies such as artificial intelligence and machine learning monitoring systems, forensic auditing and biometric verification reveals further deficiencies related to the problem with the ability dimension of fraud. In this context, persons who have skills and special access may continue to have an opportunity to commit and hide fraud cases, especially those associated with cybercrime, which was recognized as one of the most destructive frauds by respondents.

In accordance with Fraud Deterrence Theory (Beccaria, 1764; Bentham, 1789; Wells, 2014), it can be seen that deterrence systems may become ineffective due to a lack of confidence in their effectiveness rather than the absence of any reporting structures. While the majority of banks (65.9%) have reporting mechanisms in place, they are relatively infrequently used (only 48.8%). The reasons behind it were the fear of victimization, confidentiality concerns and weak sanctions for the offenders. Therefore, it can be concluded that if people have no guarantees of security or penalties for offenders, they are unlikely to use reporting tools.

Finally, the results coincide with the Fraud Management Lifecycle Theory (Hofmann, 2008). This theory advocates that fraud management is a continuous process where there should be deterrence, prevention, detection, investigation and policy improvements. All the stages of this lifecycle were

reflected in respondents' recommendations. The recommended interventions were the use of strong ethical leadership and disciplinary procedures for deterring fraud, prevention measures such as segregation of duties, multi-factor authentication and biometric authentication, as well as the development of better fraud detection measures like artificial intelligence, behavioral analysis and real-time monitoring alerts. Additionally, respondents advocated for better forensic investigation measures and regulation measures through the Reserve Bank of Zimbabwe (RBZ) supervisory measures and centralized fraud reporting measures. However, the findings show that commercial banks in Harare seem to have relatively stronger measures in deterrence and prevention rather than detection and investigation measures. The low level of implementation and effectiveness of data analytics, artificial intelligence monitoring and forensic audit suggest serious deficiencies in detecting and investigating fraud cases and learning from them in order to improve the future policies.

4.9.5 Challenges and Strategies for Improvement

Indeed, some of the most serious problems that can be identified are fast changes in technology, insider collusion, weak ethical culture and increasingly sophisticated cyber criminals. These are not distinct issues since each of them is interconnected. Firstly, it is difficult for banks to have enough money to develop technologies required to deal with fast evolving frauds. Secondly, weak cultural and governance environment can prevent control systems intended to prevent insider collusion. All these problems were also noticed by respondents, who suggested using multiple solutions including investment in technologies, strengthening governance and accountability, enhancing training and cooperation within the industry through regulation cooperation.

These suggestions are also confirmed by experiences of other countries such as South Africa and Nigeria, where better practices of auditing, whistleblower programs and information exchange between organizations proved to be very useful. All of these conclusions become the basis for the recommendations provided in Chapter Five (Owolabi & Dada, 2013; PwC Africa, 2020)..

4.10 Chapter Summary

In this chapter, the answers from 41 participants (representing an 82% response rate) taken from the compliance, audit, risk, IT security and fraud investigation departments of three banks based in Harare were considered. In terms of results, identity theft, card fraud and cyber fraud are the most frequent types of fraud while two-thirds of participants confirmed an increase in their occurrences within the last three years. At the same time, cyber fraud and insider fraud were indicated as the most costly types of fraud despite their relatively low frequency.

The fundamental anti-fraud measures such as separation of duties, authorizations, and internal audit are used almost invariably while AI-based analysis, data analysis and biometric methods are used more rarely. Overall, all the anti-fraud measures were considered as being moderately effective by the respondents who mostly agreed that the measures work but found them to be insufficiently effective. Surprisingly enough, employees consider that these measures affect customer confidence and regulatory compliance more than fraud prevention.

The most important issues noted were changing technology, collusive behavior by insiders, poor ethics and the sophistication of cyber criminals. This was emphasized by open ended questions, which showed resource constraints, cultural issues and fear of reporting as some of the key issues. All these findings using theories like the Fraud Triangle, Fraud Diamond, Fraud Deterrence and Fraud Management Lifecycle provide the foundation for conclusions and recommendations to be discussed in Chapter Five.

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter marks the end of the study on assessing the efficiency of anti-fraud measures within commercial banks in Harare, Zimbabwe. It covers the study summary, the key findings based on the analyzed data, the conclusions drawn based on the stated research objectives, as well as the recommendations formulated based on the findings. It brings the findings back to the research problem stated in Chapter One and the literature review provided in Chapter Two. In addition, it outlines several recommendations that can be applied in practice by commercial banks, regulatory bodies, and other stakeholders interested in preventing fraud and financial crimes in Zimbabwe.

5.2 Summary of the Study

The objective of the study was to assess the effectiveness of the fraud prevention measures implemented by the commercial banks in Harare, Zimbabwe. Fraud is a growing problem in the banking industry and the rising number of cases of fraud has raised questions regarding the effectiveness of fraud prevention and detection measures in commercial banks. The objectives of the study were:

- To identify the common types of fraud encountered in commercial banks in Harare.
- To assess the anti-fraud measures currently implemented by commercial banks.
- To evaluate the effectiveness of anti-fraud measures in preventing and detecting fraud.

- To identify the factors affecting the effectiveness of anti-fraud measures.
- To recommend strategies for improving anti-fraud systems in commercial banks.

A descriptive research methodology was employed in the study, along with quantitative methods. A questionnaire was structured and distributed among bank employees who work in fraud prevention, compliance, risk management, internal auditing and IT security in selected commercial banks in Harare. Of the sample size considered, 41 employees responded to the survey, thus resulting in a response rate of 82%.

The results indicated that some of the most prevalent types of frauds committed against commercial banks included identity theft, card fraud and cyber fraud. Yet, cyber fraud and insider frauds were considered to be those responsible for causing the biggest financial damages to banks since they involve very sophisticated attacks and insiders' participation.

It was also found out that a lot of commercial banks use conventional approaches to fighting frauds such as separation of duties, authorization practices, internal audit, fraud training programs and whistleblower practices. However, advanced technologies such as artificial intelligence, machine learning systems, forensic audits and biometric verification have not been employed yet.

Moreover, the research revealed that the anti-fraud mechanisms of the commercial banks are moderately efficient. Although the majority of the participants agreed that the anti-fraud mechanism contributes greatly to the building of customer's confidence and compliance to the law, the majority admitted that the efficiency of the anti-fraud measure in stopping the sophisticated fraud is not very high due to the technological advancement and collusion.

It was also discovered that the fast advancement of technology, the increased level of sophistication among the criminals, lack of adequate training of the personnel, collusion and the outdated anti-fraud detection system decrease the efficiency of the anti-fraud mechanisms.

5.3 Conclusions

Based on the findings of the study, the following conclusions were drawn:

5.3.1 Common Types of Fraud in Commercial Banks

It was found that fraud is still a great problem facing the commercial banks operating in Harare, with the frequent occurrences of fraud being identity theft, card fraud, and cyber fraud. However, it was noted that the most damaging fraud cases are cyber fraud, insider fraud, and business email compromise. This implies that although some fraud may be common, technologically enabled fraud and insider fraud is financially more damaging.

5.3.2 Anti-Fraud Measures Implemented in Commercial Banks

It was concluded that the commercial banks in Harare had put in place substantial efforts towards anti-fraud mechanisms. Almost all the banks in question have adopted basic anti-fraud mechanisms including segregation of duties, authorizations, internal audits, and employee fraud prevention programs. On the other hand, adoption of new fraud prevention mechanisms like artificial intelligence, behavioral analysis, and biometrics is still rare and is limited by cost and infrastructure challenges.

5.3.3 Effectiveness of Anti-Fraud Measures

The study came to the conclusion that the anti-fraud strategies implemented in commercial banks are somewhat effective. Even though the implementation of anti-fraud strategies has had an impact on the prevention of fraud, customer confidence and compliance issues, such measures have been unable to cope with the sophistication of fraud challenges.

5.3.4 Factors Affecting the Effectiveness of Anti-Fraud Measures

It was found out that there are a number of issues that can decrease the efficiency of the anti-fraud system. These are rapid development of technology, lack of training, poor ethics, collusion, as well as old-fashioned technology and financial difficulties to use the sophisticated anti-fraud technologies. Moreover, there is no efficient law enforcement, and fear of victimization discourages the whistle-blowing process.

5.3.5 Contribution of Anti-Fraud Measures to Banking Operations

The study revealed that anti-fraud systems serve an important purpose other than preventing frauds. The respondents were strongly of the opinion that the anti-fraud systems help build customer trust, improve regulatory compliance, and ultimately, boost the reputation of commercial banks. Hence, anti-fraud systems need to be considered as something more than just risk management systems.

5.4 Recommendations

In light of the findings and conclusions of the study, the following recommendations are made:

5.4.1 Investing in Anti-Fraud Technology

Commercial banks should invest more in anti-fraud technology like artificial intelligence, machine learning, real-time transaction monitoring system, and biometric verification. This will enhance the ability of the bank to detect suspicious transaction and reduce the need for fraud review manually.

5.4.2 Employee Training

Commercial banks should engage in the process of training their employees regularly and continuously regarding fraud awareness. The training should cover fraud trends, cyber-

attack, phishing, insider fraud and social engineering. They should encourage scenario-based training where real life fraud is used.

5.4.3 Implementation of Strict Internal Controls

The commercial bank should enforce separation of duties, job rotation in sensitive departments and authorization. They should perform surprise audits as well as continuous monitoring of privileged users to prevent insider fraud.

5.4.4 Creation of a Robust Ethical Culture

The commercial banks should encourage an ethical culture among its employees through practicing integrity and accountability in all processes. This will involve strengthening the confidential whistleblower system where employees can easily report suspicious activities without being victimized.

5.4.5 Improved Collaboration between Banks and Regulators

Commercial banks must enhance cooperation with the Reserve Bank of Zimbabwe, law enforcement agencies, and financial institutions in exchanging information about any potential threats, such as fraud. Fraud reporting should be done to the extent of building an intelligence database on those offenders who commit fraud across different institutions.

5.4.6 Better Regulatory Enforcement

Regulatory body, such as Reserve Bank of Zimbabwe, needs to develop and monitor compliance of commercial banks through enhanced supervisory inspection. It is also required to create anti-fraud standards which commercial banks have to follow. Better prosecution of offenders can further decrease the amount of committed fraud.

5.4.7 Customer Awareness Programs

Customer awareness programs need to be implemented in terms of educating customers about any emerging threats using SMSs, mobile banking, social networks, and branches.

5.5 Areas for Further Research

This study focused on commercial banks in Harare, Zimbabwe. Further studies may be conducted in the following areas:

- A comparative analysis of the effectiveness of anti-fraud strategies in local versus foreign banks in Zimbabwe.
- An evaluation of the role played by artificial intelligence and machine learning in fraud detection in banks in Zimbabwe.
- An analysis of customer awareness and how it affects fraud prevention in the banking industry.
- An analysis of the link between organizational culture and insider fraud in financial institutions.

5.6 Chapter Summary

This chapter has summarized the findings of the research as well as conclusions and recommendations. It has been revealed that despite the use of a number of anti-fraud techniques in commercial banks in Harare, fraud continues to be a significant problem owing to changing technology, internal problems, and insufficient resources. Although current efforts prove to be moderately effective, there is a need for further improvement in technology, training, governance, customer awareness and coordination in order to make fraud prevention and detection more effective.

REFERENCES

- African Union. (2021). *Combating Illicit Financial Flows in Africa*. Addis Ababa: African Union Commission.
- Albrecht, W. S. (2019). Fraud: The Ultimate Challenge for Financial Institutions. *Journal of Financial Crime*, 26(3), 726-742.
- Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2016). *Fraud Examination* (5th ed.). Boston: Cengage Learning.
- Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2020). *Fraud Examination* (6th ed.). Boston: Cengage Learning.
- American Institute of Certified Public Accountants (AICPA). (2019). *Internal Control and Fraud Prevention*. New York: AICPA.
- Aremo, A. G., Oder, R. O., & Beasley, M. S. (2020). The Role of Auditing in Fraud Prevention and Detection. *International Journal of Auditing*, 24(2), 187-203.
- Arens, A. A., Elder, R. J., & Beasley, M. S. (2020). *Auditing and Assurance Services: An Integrated Approach* (17th ed.). Boston: Pearson.
- Association of Certified Fraud Examiners (ACFE). (2020). *Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse*. Austin, TX: ACFE.
- Association of Certified Fraud Examiners (ACFE). (2022). *Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse*. Austin, TX: ACFE.
- Association of Certified Fraud Examiners (ACFE). (2024). *Report to the Nations: 2024 Global Study on Occupational Fraud and Abuse*. Austin, TX: ACFE.
- Babbie, E. (2016). *The Practice of Social Research* (14th ed.). Boston: Cengage Learning.
- Basel Committee on Banking Supervision. (2018). *Sound Practices for the Management and Supervision of Operational Risk*. Basel: Bank for International Settlements.

- Beauchamp, T. L., & Childress, J. F. (2013). *Principles of Biomedical Ethics* (7th ed.). New York: Oxford University Press.
- Beccaria, C. (1764). *On Crimes and Punishments*. Milan: Unknown Publisher.
- Bentham, J. (1789). *An Introduction to the Principles of Morals and Legislation*. London: T. Payne and Son.
- Bologna, J. (2018). *Fraud and Embezzlement in Financial Institutions*. New York: Routledge.
- Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2), 77-101.
- Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, CA: Praeger.
- British Educational Research Association (BERA). (2018). *Ethical Guidelines for Educational Research* (4th ed.). London: BERA.
- British Standards Institution (BSI). (2019). *Data Protection and Privacy Guidelines*. London: BSI.
- Brotby, W. K. (2009). *Information Security Management Metrics*. Boca Raton, FL: CRC Press.
- Brown, J. (2021). *Fraud Detection and Prevention in Financial Institutions*. London: Palgrave Macmillan.
- Bryman, A. (2016). *Social Research Methods* (6th ed.). Oxford: Oxford University Press.
- Button, M. (2014). *Fraud and Financial Crime*. London: Routledge.
- Button, M., & Gee, J. (2013). *Countering Fraud for Competitive Advantage*. London: Wiley.
- Capras, I., & Achim, M. V. (2024). Corporate Fraud in Romania: An Empirical Analysis. *Journal of Financial Crime*, 31(1), 156-175.
- Chambers, J., & Dhiraj, A. (2020). *Data Analytics for Fraud Detection*. New York: Springer.
- Chitsora, T. (2023). Fraud Typologies in Zimbabwean Banks: A Case Study of Selected Commercial Banks. *Zimbabwe Journal of Financial Crime*, 12(2), 45-67.

- Coalition Against Insurance Fraud. (2020). Insurance Fraud: The Hidden Cost. Washington, DC: Coalition Against Insurance Fraud.
- Cressey, D. R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Glencoe, IL: Free Press.
- Creswell, J. W. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Thousand Oaks, CA: SAGE Publications.
- Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Thousand Oaks, CA: SAGE Publications.
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and Conducting Mixed Methods Research* (3rd ed.). Thousand Oaks, CA: SAGE Publications.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). Thousand Oaks, CA: SAGE Publications.
- Derrig, R. A. (2002). Insurance Fraud. *Journal of Insurance Regulation*, 21(1), 47-73.
- Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method* (4th ed.). Hoboken, NJ: Wiley.
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4.
- Federal Bureau of Investigation (FBI). (2020). *Financial Crime Report*. Washington, DC: FBI.
- Federal Trade Commission. (2020). *Identity Theft: A Guide for Consumers*. Washington, DC: FTC.
- Ferraiolo, D., Kuhn, D. R., & Gavrila, S. (2015). *Access Control and Authorization*. Gaithersburg, MD: National Institute of Standards and Technology.
- Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving Integration in Mixed Methods Designs—Principles and Practices. *Health Services Research*, 48(6pt2), 2134-2156.
- Field, A. (2018). *Discovering Statistics Using IBM SPSS Statistics* (5th ed.). London: SAGE Publications.

- Financial Action Task Force (FATF). (2020). Guidance on Anti-Money Laundering and Counter-Terrorist Financing. Paris: FATF.
- Financial Intelligence Unit (FIU). (2021). Annual Report on Financial Crime in Zimbabwe. Harare: FIU.
- Flowerastia, F., Setiawan, A., & Putri, A. (2021). The Role of Internal Control and Fraud Awareness in Fraud Prevention. *Journal of Financial Crime*, 28(4), 987-1003.
- Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2012). *How to Design and Evaluate Research in Education* (8th ed.). New York: McGraw-Hill.
- George, D., & Mallery, P. (2003). *SPSS for Windows Step by Step: A Simple Guide and Reference* (4th ed.). Boston: Allyn & Bacon.
- Grafton Library. (2024). *Research Methods: Primary and Secondary Data*. Winchester, VA: Grafton Library.
- Gwaka, T. (2024). Effectiveness of Anti-Fraud Measures in ZB Bank Bindura. *Bindura University Journal of Commerce*, 8(1), 34-52.
- Halliday, J., Badenhorst, J., & Solms, R. V. (2012). Authentication Mechanisms in Banking. *Journal of Information Security*, 3(2), 112-126.
- Haynes, S. N., Richard, D. C., & Kubany, E. S. (1995). Content Validity in Psychological Assessment. *Psychological Assessment*, 7(3), 238-247.
- Hofmann, W. (2008). *The Fraud Management Lifecycle*. London: Sage Publications.
- Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM*, 55(1), 74-81.
- Institute of Internal Auditors (IIA). (2020). *International Standards for the Professional Practice of Internal Auditing*. Altamonte Springs, FL: IIA.
- Internal Revenue Service (IRS). (2020). *Tax Evasion and Fraud*. Washington, DC: IRS.
- International Auditing and Assurance Standards Board (IAASB). (2020). *International Standards on Auditing*. New York: IFAC.
- Irwin, A. (2018). *Electronic Card Fraud: Threats and Solutions*. London: Routledge.

- Israel, M., & Hay, I. (2006). *Research Ethics for Social Scientists*. London: SAGE Publications.
- Jenkins, D. (2020). *Financial Statement Fraud: Detection and Prevention*. New York: Wiley.
- Jones, M. (2022). Phishing and Identity Theft: Emerging Trends. *Cybersecurity Journal*, 15(3), 234-251.
- KPMG Africa. (2021). *Banking Fraud Survey 2021*. Johannesburg: KPMG.
- Krutikov, A., & Graycar, A. (2018). Employee Awareness and Fraud Prevention. *Journal of Financial Crime*, 25(3), 698-714.
- Leedy, P. D., & Ormrod, J. E. (2019). *Practical Research: Planning and Design* (12th ed.). Boston: Pearson.
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Beverly Hills, CA: SAGE Publications.
- Lind, D. A., Marchal, W. G., & Wathen, S. A. (2017). *Statistical Techniques in Business and Economics* (17th ed.). New York: McGraw-Hill.
- Mabika, T. (2015). Fraud in Zimbabwean Local Authorities: Causes and Consequences. *Zimbabwe Journal of Public Administration*, 7(2), 45-68.
- Malle, S., Mwangi, P., & Mwenda, J. (2021). Factors Influencing Fraud Prevention in Tanzania's Public Sector. *African Journal of Financial Crime*, 9(1), 78-96.
- Mandizvidza, C., Moyo, T., & Ndlovu, S. (2020). Forensic Auditing in Zimbabwe: Challenges and Opportunities. *Journal of Forensic Accounting*, 12(1), 23-45.
- Manhide, T., & Nkomo, L. (2023). Electronic Banking Fraud in Zimbabwe: Trends and Countermeasures. *Zimbabwe Journal of Banking and Finance*, 15(2), 67-89.
- Mashayanye, P. (2015). The Role of Forensic Auditing in Fraud Detection in Zimbabwean Banks. *Journal of Accounting and Finance*, 10(3), 134-156.
- Messmer, M. (2020). Job Rotation as a Fraud Prevention Strategy. *Journal of Corporate Governance*, 16(2), 89-105.
- Mohammed, A., Asokan, R., & Arunasalam, R. (2023). Digital Forensic Tools and Corporate Policies in Combating Financial Fraud. *Journal of Financial Crime*, 30(2), 456-475.

- Morrison, J. (2020). *Fraud Prevention Training and Awareness*. London: Routledge.
- Munyanyi, T. (2022). Cyber Fraud in African Banking: Challenges and Solutions. *African Journal of Information Security*, 11(4), 234-259.
- Mutambirwa, S., Moyo, A., & Chirisa, T. (2022). Fraud Detection in Zimbabwean Industry: The Role of Internal Auditing. *Journal of Accounting and Finance*, 18(3), 112-134.
- Mutanda, T., & Maireva, C. (2023). Cyber Fraud Strategies in Zimbabwean Banks: An Evaluation. *Zimbabwe Journal of Financial Crime*, 14(1), 34-56.
- National Institute of Standards and Technology (NIST). (2015). *Access Control and Authorization Guidelines*. Gaithersburg, MD: NIST.
- Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches* (7th ed.). Boston: Pearson.
- Ogunode, O., & Dada, A. (2022). Fraud Prevention Strategies in Nigerian Banks. *Journal of Financial Crime*, 29(3), 567-589.
- Okoye, E., & Gbegi, D. (2013). Internal Control and Fraud Prevention in Nigerian Banks. *Journal of Accounting and Financial Management*, 5(2), 45-68.
- Owolabi, S., & Dada, A. (2013). Internal Audit and Fraud Prevention in Nigerian Banks. *Journal of Financial Crime*, 20(4), 389-406.
- Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), 533-544.
- Pallant, J. (2020). *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using IBM SPSS* (7th ed.). London: Routledge.
- Penn Audit, Compliance and Privacy. (2020). *Segregation of Duties: Best Practices*. Philadelphia, PA: Penn Audit.
- PwC Africa. (2020). *Global Economic Crime and Fraud Survey 2020: Africa Report*. Johannesburg: PwC.

- Ramamoorti, S., Morrison, J., & Koletar, J. (2020). *Hiring Practices and Fraud Prevention*. New York: Routledge.
- Ramsay, R. J. (2020). *Compliance Auditing: Principles and Practice*. London: Sage.
- Rashid, M., Agrawal, R., & Sharma, M. (2022). Data Analytics in Fraud Detection. *Journal of Business Analytics*, 5(2), 123-145.
- Reserve Bank of Zimbabwe (RBZ). (2022). *Annual Banking Supervision Report*. Harare: RBZ.
- Reserve Bank of Zimbabwe (RBZ). (2023). *Annual Banking Supervision Report*. Harare: RBZ.
- Reserve Bank of Zimbabwe (RBZ). (2025). *Commercial Banking Sector Statistics*. Harare: RBZ.
- Resnik, D. B. (2015). What Is Ethics in Research and Why Is It Important? *National Institute of Environmental Health Sciences*, 12(3), 45-67.
- Reuters. (2024). *Fraud Risk Management in Financial Institutions*. London: Thomson Reuters.
- Reurink, A. (2016). Financial Fraud: A Review of the Literature. *Journal of Economic Surveys*, 30(4), 712-743.
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* (8th ed.). Harlow: Pearson Education.
- Securities and Exchange Commission (SEC). (2020). *Ponzi Schemes and Investment Fraud*. Washington, DC: SEC.
- Shungu, S., & Mabuyaye, M. (2024). Data Analytics and Fraud Detection in Zimbabwean Banks. *Journal of Financial Analytics*, 9(1), 45-68.
- Smith, J., & Jones, M. (2023). *Data Analysis and Quality Control in Social Research*. London: Routledge.
- Tavakol, M., & Dennick, R. (2011). Making Sense of Cronbach's Alpha. *International Journal of Medical Education*, 2, 53-55.
- Trevino, L. K., & Nelson, K. A. (2017). *Managing Business Ethics: Straight Talk About How to Do It Right* (7th ed.). Hoboken, NJ: Wiley.

- Trochim, W. M. K., & Donnelly, J. P. (2006). *The Research Methods Knowledge Base* (3rd ed.). Mason, OH: Atomic Dog Publishing.
- Van Teijlingen, E. R., & Hundley, V. (2001). The Importance of Pilot Studies. *Social Research Update*, 35, 1-4.
- Wang, X. (2016). Motivations for Fraud: A Review of the Literature. *Journal of Financial Crime*, 23(1), 56-78.
- Wells, J. T. (2014). *Principles of Fraud Examination* (4th ed.). Hoboken, NJ: Wiley.
- Wells, J. T. (2017). *Corporate Fraud Handbook: Prevention and Detection*. Hoboken, NJ: Wiley.
- Wells, J. T. (2020). *Principles of Fraud Examination* (5th ed.). Hoboken, NJ: Wiley.
- Wells, J. T. (2024). *Fraud Examination: Theory and Practice*. Hoboken, NJ: Wiley.
- Wells, J. T., & Rose, J. (2016). *Hiring Practices and Fraud Prevention*. New York: Routledge.
- Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Boston: Cengage Learning.
- Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal*, 74(12), 38-42.
- Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2019). *Business Research Methods* (10th ed.). Boston: Cengage Learning.

APPENDIX A

CONSENT SECTION

Before you begin, please confirm your voluntary participation:

- ☐ Yes, I voluntarily agree to participate in this study.
- ☐ No, I do not wish to participate. (If no, please return blank.)

If you agree, please complete the questionnaire. You may skip any question or withdraw at any time without penalty.

SECTION A: DEMOGRAPHIC INFORMATION

Please tick (✓) or circle the appropriate option.

A1. Gender

- ☐ Male
- ☐ Female
- ☐ Non-binary
- ☐ Prefer not to say

A2. Age group

- ☐ 20–29 years
- ☐ 30–39 years
- ☐ 40–49 years
- ☐ 50+ years

A3. Highest qualification

- ☐ Diploma
- ☐ Bachelor's
- ☐ Master's
- ☐ Professional certification
- ☐ Other (please specify) _____

A4. Your role / functional area (choose the one that best fits)

- ☐ Compliance
- ☐ Internal Audit
- ☐ Risk Management
- ☐ IT Security
- ☐ Fraud Investigation/Financial Intelligence
- ☐ Other (please specify)_____

A5. Years of experience in banking / financial services

- ☐ Less than 2 years
- ☐ 2–5 years
- ☐ 6–10 years
- ☐ More than 10 years

A6. Types of institutions

- ☐ Local commercial bank
- ☐ Foreign-owned commercial bank
- ☐ Building society
- ☐ Other _____

SECTION B: TYPES OF FRAUD ENCOUNTERED

Based on your personal knowledge or observation in the past 12 months.

B1. Which of the following fraud types have you observed or been aware of in your bank? (Tick all that apply)

- ☐ Identity theft/impersonation
- ☐ Cheque fraud
- ☐ Card fraud (ATM skimming, card cloning, POS fraud)
- ☐ Loan fraud (false documentation, misrepresentation)
- ☐ Insider fraud/employee collusion (unauthorised transactions, embezzlement)
- ☐ Cyber fraud (phishing, vishing, business email compromise, API attacks)
- ☐ Money laundering through customer accounts
- ☐ Financial statement fraud (manipulation of records)
- ☐ Other (please specify): _____

B2. Frequency of fraud incidents:

- ☐ Less than once per month
- ☐ 1–5 per month
- ☐ 6–10 per month
- ☐ More than 10 per month
- ☐ Unsure

B3. Compared to three years ago, fraud incidents have:

- ☐ Increased significantly
- ☐ Increased slightly
- ☐ Remained same
- ☐ Decreased slightly
- ☐ Decreased significantly

B4. In your opinion, which single fraud type has caused the greatest financial loss to your bank in the last three years?

SECTION C: ANTI-FRAUD MEASURES CURRENTLY IMPLEMENTED

C1. Which of the following anti-fraud measures are currently in place in your bank? (Tick all that apply)

- ☐ Segregation of duties

- ☐ Job rotation for sensitive roles
- ☐ Formal authorization/approval processes for transactions
- ☐ Data analytics / automated fraud detection software
- ☐ Robust hiring practices (background checks, reference verification)
- ☐ Mandatory fraud awareness training for employees
- ☐ Multi-factor authentication
- ☐ Biometric verification
- ☐ Artificial intelligence (AI) / machine learning monitoring systems
- ☐ Customer transaction alerts
- ☐ Cybersecurity awareness programs for employees
- ☐ Regular internal audits focused on fraud risks
- ☐ Whistleblowing hotline / confidential reporting channel
- ☐ Forensic auditing capabilities
- ☐ Incident response plan for fraud
- ☐ Other (please specify): _____

C2. How often does your bank provide formal fraud awareness training to staff?

- ☐ Never
- ☐ Once a year
- ☐ Twice a year

☐ Quarterly

☐ More than quarterly

C3. Does your bank have a whistleblowing mechanism (e.g., anonymous hotline, online portal)?

☐ Yes, and it is actively used

☐ Yes, but it is rarely used

☐ No

☐ I don't know

SECTION D: PERCEIVED EFFECTIVENESS OF ANTI-FRAUD MEASURES

Please indicate how effective you believe EACH measure is in detecting or preventing fraud in your bank.

(1 = Not effective at all/Never used, 5 = Extremely effective/Always used)

Anti-fraud measure	Effectiveness (1-5)				Frequency of use (1-5)			
Segregation of duties	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			
Job rotation	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			
Forensic auditing	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			

Fraud awareness training	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			
Internal audits	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			
Whistleblowing hotline	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			
Background checks/robust hiring	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			
Authorized/approval processes	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			
Data analytics/automated monitoring	1 ☐	2 ☐	3 ☐	4 ☐	1 ☐	2 ☐	3 ☐	4 ☐
	5 ☐				5 ☐			

D10. Overall, how effective do you find the current anti-fraud measures in your bank?

- ☐ Very ineffective
- ☐ Somewhat ineffective
- ☐ Neither effective nor ineffective
- ☐ Somewhat effective
- ☐ Very effective

D11. To what extent do you believe anti-fraud measures contribute to customer trust in your bank?

- ☐ Not at all

- ☐ Slightly
- ☐ Moderately
- ☐ Significantly
- ☐ Don't know

D12. To what extent do anti-fraud measures assist your bank in complying with regulatory requirements (e.g., RBZ, AML/CFT)?

- ☐ Not at all
- ☐ Slightly
- ☐ Moderately
- ☐ Significantly
- ☐ Don't know

SECTION E: FACTORS AFFECTING EFFECTIVENESS

Please rate how much each factor limits the effectiveness of anti-fraud measures in your bank.

(1 = Not a limitation, 5 = A very severe limitation)

Limited Factor	1	2	3	4	5
Outdated or weak technology/security systems	☐	☐	☐	☐	☐
Inadequate employee training and awareness	☐	☐	☐	☐	☐
Weak internal controls	☐	☐	☐	☐	☐

Limited financial resources to invest in fraud prevention	☐	☐	☐	☐	☐
An organizational culture that does not prioritize ethics	☐	☐	☐	☐	☐
Weak legal/regulatory enforcement	☐	☐	☐	☐	☐
Insider collusion across multiple departments	☐	☐	☐	☐	☐
Sophistication of cybercriminals	☐	☐	☐	☐	☐
Rapid technological change	☐	☐	☐	☐	☐
Third party/vendor vulnerabilities	☐	☐	☐	☐	☐
Limited AI/advanced detection capabilities	☐	☐	☐	☐	☐

E8. What are the biggest challenges or obstacles that limit the effectiveness of anti-fraud measures in your bank?

SECTION F: RECOMMENDATIONS & OPEN-ENDED INSIGHTS

F1. What specific actions should bank implement to improve fraud prevention and detection?

F2. Do you have any additional comments regarding anti-fraud measures in commercial banks in Harare? (Optional)
