

BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES



**THE EFFECTIVENESS OF INTERNAL CONTROLS IN UNEARTHING FRAUD IN
FINANCIAL INSTITUTIONS IN ZIMBABWE.A SURVEY OF FINANCIAL
INSTITUTIONS IN HARARE CBD. (2025-2026)**

SUBMITTED BY JOSEPH JAMES CHINHAMU

B210783B

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

SUPERVISOR_____

APPROVAL FORM

The undersigned certify that they have read and recommend Bindura University of Science Education for acceptance, a research project entitled: “THE EFFECTIVENESS OF INTERNAL CONTROLS IN UNEARTHING FRAUD IN FINANCIAL INSTITUTION IN ZIMBABWE. A SURVEY OF FINANCIAL INSTITUTION IN HARARE CBD. (2025-2026), submitted by Joseph James Chinhamu in partial fulfilment of the requirements of the Bachelor of Commerce (Honour’s) Degree in Financial Intelligence.

To be completed by student. I certify that this dissertation meets the preparation guidelines as presented in the Faculty Guide and Instructions for typing dissertations Signature of

student



Date :30 July 2026.

To be completed by supervisor. This dissertation is suitable for submission to the faculty. This dissertation should be checked for conformity with Faculty guidelines. Signature of

Supervisor:...



Date :30 July 2026

III. To be completed by Chair of Department. I certify to the best of my knowledge that the required procedures have been followed and the preparation criteria has been met for this dissertation.

Signature of Chairperson.....



..... Date...17/8/26.....

RELEASE FORM

Name of Author: Chinghamu Joseph James

Title of Project: The effectiveness of internal controls in unearthing fraud in financial institutions in Zimbabwe. A survey of financial institutions in Harare cbd

Degree Programme: Bachelor of Commerce (Honours) in Financial Intelligence

Year submitted: 2026

Permission is hereby granted to Bindura University of Science Education to produce single copies of this research project for private scholarly research purposes only.

Signed: Date:

Dedication Form

Special dedication to my parents Mr. and Mrs. Chinhamu, my siblings Joshua, Kimberly, Innocent and Maud who have always encouraged and supported me in pursuing my dreams. Your love and guidance have been my anchor and my inspiration in this endeavor. Not forgetting my best friend Vongai the unwavering support you gave me, I really appreciate your support.

ABSTRACT

This study is on the effectiveness of internal controls in unearthing fraud in the financial institutions, a survey of Harare central business district. It was informed by the following objectives; to identify the types of internal control mechanisms currently implemented by the financial institutions domicile in Harare central business district; to evaluate the extent to which these internal controls detect common fraud schemes; to determine the challenges that limit the effectiveness of internal controls in detecting fraud and to recommend the adoption of effective strategies. The study population was 120 were a sample of 92 was deduced using purposive sampling techniques. Data was gathered using questionnaires and interview guides. The data was analyzed using Atlas ti , Microsoft excel and SPSS version 27 for rating The results from the analysis was presented using tables, pie charts and bar graphs. From the study it was found that the most common fraud types identified are asset misappropriation and financial statement fraud, followed by cyber-enabled fraud and Key internal control weaknesses include insufficient technological tools, inadequate staff fraud training, management override, employee collusion, and siloed information systems. It was concluded that while internal controls partially detect fraud, significant gaps in technology, resources, and oversight remain, and from the conclusions of the study it is recommended that multi-factor authentication, real-time transaction monitoring, regular fraud training, and inter-institutional intelligence sharing.

Acknowledgements

Firstly, I want to give praises and thanks to the Lord Almighty, for his showers of blessings throughout my research work to complete it successfully. I would like to express my deep and sincere gratitude to my research supervisor Mr Gombarume for giving me the opportunity to do research and providing invaluable guidance throughout this research. Their dynamism, patience, vision, sincerity and motivation were unimaginable. I am grateful to Vongai whose support was never wavering.

Table of Contents

Table of Contents

CHAPTER 1	1
INTRODUCTION	1
1.0 Introduction.....	1
1.1 Background of study	1
1.2 Statement of problem.....	2
1.3 Purpose of the Study	3
1.4 Research objectives.....	4
1.5 Research questions.....	4
1.6 Significance of the Study	4
1.7 Assumptions of the Study	5
1.8 Delimitations of the Study	6
1.9 Limitations of the Study.....	6
1.10 Definition of terms.....	7
1.11 Summary	7
CHAPTER 2	8
LITERATURE REVIEW	8
2.0 Introduction.....	8
2.1 Conceptual Framework.....	8
2.1.1 Internal controls	8
2.1.2 Fraud	9
2.1.3 COSO framework	11
2.2 Theoretical Framework	15
2.2.1 The Fraud Triangle Theory (Cressey, 1953)	15
2.2.2 Fraud diamond theory	18
2.2.3 Control Fraud Theory	19
2.3.4 Theory of collusion.....	19
2.4 Empirical review	20
2.5 Research Gap analysis	23

2.6 Summary	24
CHAPTER 3	25
RESEARCH METHODOLOGY	25
3.0 Introduction	25
3.1 Research design	25
3.2 Target population	26
3.3 Sampling	26
3.3.1 Sampling Techniques	27
3.3.2 Sample size	27
3.4 Research instruments	28
3.4.1 Questionnaires.....	28
3.4.2 Interviews.....	29
3.4.3 Justification	30
3.4.4 Document Analysis	30
3.5 Sources of Data	31
3.5.1 Primary Data	31
3.5.2 Secondary Data	31
3.6 Data collection procedure	32
3.7 Data Presentation and Analysis.....	32
3.8 Validity and Reliability	32
3.9 Ethical Considerations	33
3.10 Summary	33
CHAPTER 4	34
DATA PRESENTATION, ANALYSIS AND DISCUSSION	34
4.0 Introduction.....	34
4.1 Response analysis	34
4.1.1 Questionnaire response rate	34
4.1.2 Response rate for interviews.....	35
4.2 Quantitative analysis	36
4.2.1 Age of respondents.....	36
4.2.2 Sector participation	37

4.2.3 Level of experience.....	38
4.2.4 Organizational departments.	39
4.2.5 Fraud typologies.....	40
4.2.6 Corporate environment in relation to internal controls.....	41
4.2.7 The effectiveness of internal controls	42
4.3 Qualitative data analysis	43
4.3.1 Internal Controls Currently in Place	43
4.3.2 Effectiveness of the current implemented internal controls.....	43
4.3.3 Challenges Limiting Effectiveness	44
4.3.4 Possible recommendations to failures of internal controls	47
4.4 Summary	48
CHAPTER 5	49
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS	49
5.0 Introduction.....	49
5.1 Summary of Major Findings.....	49
5.2 Conclusions.....	50
5.3 Recommendations.....	50
5.3.1 Recommendations for Financial Institutions	51
5.3.2 Recommendations for Future Research	53
5.4 Summary	54
References.....	55

List of tables

Table 4.1	35
Table 4.2.....	35
Table 4.3	41

List of figures

Figure 2.1. Classification of fraud	10
Figure 2.2. Coso framework.....	15
Figure 2.3. Fraud triangle	16
Figure 2.4. The fraud diamond	18
Figure 4.1. Age of respondents	36
Figure 4.2 Sector representation	37
Figure 4.3 Level of experience	38
Figure 4.4 Organizational departments	39
Figure 4.5 Fraud typologies	40
Figure 4.6 The effectiveness of internal controls	42
Figure 4.7 Fraud risk assessment	45

LIST OF APPENDICES

APPENDIX 1: RESEARCH ASSISTANCE LETTER.....	61
APPENDIX 2: QUESTIONNAIRE FOR FINANCIAL INSTITUTIONS STAFF	62
APPENDIX 3: INTERVIEW GUIDE.....	67
APPENDIX 4: TURNITIN REPORT	68

ABBREVIATIONS

FIU – Financial Investigation Unit

RBZ – Reserve Bank of Zimbabwe

STRs- Suspicious Transaction Reports

CBD- Central Business District

ACFE- Association of Certified Fraud Examiners

FCA -Financial Conduct Authority (UK financial regulator)

CHAPTER 1

INTRODUCTION

1.0 Introduction

This chapter introduces background to the study, statements of the problem, research objectives and purpose of the study and significance of the study. Assumptions, delimitations, hypothesis, limitations and definition of terms are at the end of the chapter.

1.1 Background of study

The stability and integrity of any national economy are fundamentally anchored on the soundness of its financial system. In Zimbabwe, the financial sector serves as the critical engine for resource mobilization, capital allocation and facilitation of domestic and international trade. However, the pervasive threat of financial fraud has persistently undermined the stability, eroded public trust and imposed significant economic costs. Gee and Button, (2019) also pointed ‘that the global fraud losses are equivalent to 6.05% of GDP, that is, \$5.127 trillion, while related losses have increased by 56% in the last decade’. Hence the devastating effects of fraud have resulted in internal control gaining more grounds over the years. This can be drawn from the corporate and accounting scandals of the past like the Enron, WorldCom and Tyco scandals in 2002, costing investors to lose billions of dollars and resulting in the enactment of the Sarbanes–Oxley Act, also known as SOX (Sarbanes & Oxley, 2002). The legislative reason behind the internal control requirements in the Sarbanes Oxley Act of 2002 (SOX) ‘was to reduce the possibility of corporate misconduct and fraud and to curtail corporate insiders' ability to do fraud’ (Gao & Jia, 2015).

In Kenya there is the Goldenberg scandal involving roughly 600 million dollars to over 2 billion dollars in fraudulent payments for non-existent gold and diamond exports “Death of a whistle blower” (Mambo Africa .27 September,2010). A substantial amount of money was taken into private hands and deprive the general public and thus made the country reputation fall below par

standards regionally. In such a context, it is certainly necessary to have fraud prevention, detection, analysis and management systems for the reliability of published financial performance information and consequently for the continuity and stability of activities. In particular, the internal control system is supposed to enable companies to better mitigate the risks of fraud and to face new challenges relating to new technologies. Cuomo, (2005).

In the past Zimbabwe has faced its fate on fraudulent financial activities the like of Barbican bank and Time bank they were involved in abusing of deposit funds and engaging in illegal foreign currency dealings. The Herald, (2013). Despite the theoretical primacy of internal controls, financial institutions in Zimbabwe continue to experience significant fraud-related challenges. Internal controls in Zimbabwean banks were notably weak, a finding that remains pertinent today. Tembo, (2015). In a more recent assessment, the Financial Intelligence Unit (FIU) of Zimbabwe, the primary regulatory body responsible for supervising financial institutions for anti-money laundering and counter-terrorist financing compliance (FIU) reported that between February and April 2024, four banks were penalized for serious deficiencies in customer due diligence, transaction monitoring, and sanctions compliance (FIU, 2024). The FIU further estimated that predicate crimes including fraud, generated illicit proceeds equivalent to approximately US\$1.23 billion annually (FIU, 2024). These regulatory findings indicate that the gap between the theoretical design of internal controls and their operational effectiveness remains a critical concern.

The persistence of fraud, is evidenced by recent high-profile cases such as the US\$34,500 cyber-enabled fraud perpetrated against the Reserve Bank of Zimbabwe (RBZ) itself (Nehanda Radio, 2025), raises profound questions about the efficacy of the current control regimes. While numerous studies have examined internal controls in Zimbabwean financial institutions (Njanike et al., 2011; Tembo, 2015),

1.2 Statement of problem

Zimbabwe's financial sector is regulated with laws that hinder the occurrence of fraud such as the Money laundering and proceeds of crime act (chapter 9:24), securities and exchange act (chapter 24:25) and the Banking act (chapter 24:20). (Constitution of Zimbabwe). Although fraud continue to occur threatening stability and integrity of the national payment system. The financial service sector organizations have their own code of ethics which guide how work is done prohibiting the

occurrence of fraud in their operations. Despite the presence of regulatory frameworks and internal control policies mandated by the Reserve Bank of Zimbabwe and the Financial Intelligence Unit. Fraud incidences continue to manifest in various forms including cyber-enabled fraud, related party transaction abuses, money laundering, asset misappropriations and foreign exchange market manipulation. Enforcement actions and prosecutions for financial crimes fall short of demonstrating an effective national anti-money laundering and counter-terrorist financing system, a warning that places the country at risk of failing future international evaluations. Kapesa, (2026); FIU, (2024); RBZ, (2025). The FIU (2024). A fundamental disconnection appears to exist between the existence of control mechanisms and their practical capability to detect fraudulent activities. This problem is particularly acute because previous research, such as that by Tembo (2015), has identified weak internal controls as a primary cause of fraud in Zimbabwean banks, yet there is a scarcity of empirical studies assessing the contemporary effectiveness of these controls specifically from the vantage point of the key regulatory authority the FIU. Without such an assessment, the specific deficiencies within the control environment, risk assessment or monitoring activities that impede fraud detection remain unknown, thereby hindering the development of targeted and effective policy interventions. This study therefore seeks to systematically investigate the relationship between the effectiveness of internal controls and the detection of fraud in Zimbabwean financial institutions. Another view will be to ascertain the facts of the study Fraud Detection. This is defined as the ability of an organization to identify, uncover and report instances of financial fraud measured by indicators such as the number and value of fraud cases detected, suspicious transaction reports (STRs) generated and successful enforcement actions.

1.3 Purpose of the Study

The main purpose of the study was to establish the effectiveness of internal controls in uncovering fraud within the financial service sector focusing more on Harare central business district because of the volume of financial transactions conducted daily. It was motivated by the persistent and escalating challenge of fraud in the financial sector which have inflicted to much losses and eroded the public confidence in the country banking system. Reports indicate a surge in fraud incidents with \$6.15 billion lost from 2019 to 2024 and annually losing to about \$1.23 billion thus about 3.4 % of the Zimbabwe GDP. According to FIU fraud accounts for about 500 million annually as a key driver of dirty money.

1.4 Research objectives

The study was guided by the following objectives;

- To identify the types of internal control mechanisms currently implemented by the financial institutions domicile in Harare central business district.
- To evaluate the extent to which these internal controls detect common fraud schemes.
- To determine the challenges that limit the effectiveness of internal controls in detecting fraud.
- To recommend the adoption of effective strategies.

1.5 Research questions

- i. What types of internal control systems are in place at financial institutions domicile in Harare central business district?
- ii. How effective are these internal controls in detecting fraud?
- iii. What are the major challenges suffocating internal controls from effectively detecting fraud?
- iv. Is there a significant relationship between specific internal control activities and the frequency in the detection of fraud?
- v. What measures can be adopted to enhance the fraud detection role of internal controls in financial institutions in central business district of Harare?

1.6 Significance of the Study

i. To the researcher

Studying fraud equips students with valuable knowledge and skills related to fraud, digital forensics, risk management, and incident response. This knowledge is highly sought-after in today's job market, as organizations across various industries seek professionals with expertise in combating fraud threats. Additionally, a student who is studying for a Bachelor of Commerce Honors degree in Financial Intelligence can work on various post like fraud analytics, digital forensics investigating, security consulting, incident or policymaking. These career paths offer excellent job prospects, competitive salaries and chances for professional growth.

ii. To the nation

This study is expected to give a substantial contribution to policy, practice and academic literature. From a practical and policy perspective, the findings will provide the financial sector community with empirical evidence to identify specific weaknesses in the internal controls. This can inform particular supervisory guidance, enforcement priorities and the design of more effective AML/CFT regulations particularly as the country prepares for its international evaluation. The results will offer a benchmark for self-assessment highlighting which control measures require urgent strengthening to enhance their fraud detection capabilities and avoid regulatory penalties.

iii. To the university

From an academic perspective, this study contributes to the limited body of empirical research on internal control effectiveness in developing economy financial sectors, specifically within the unique and challenging Zimbabwean context. It tests its predictive power regarding fraud detection, extending the work of scholars such as Njanike et al. (2011) and Kanu et al. (2025). The gathered information will be used by other researchers for source of information to strengthen their further researches.

1.7 Assumptions of the Study

The assumption below informed this study;

The participants will voluntarily provide information. It is also assumed that respondents from the Financial Institutions, who are professionals in financial operations and compliance will provide honest, accurate and unbiased responses to the survey questionnaire. The internal control systems in place at the financial institutions under the FIU's purview can be reliably assessed. It is also assumed that the data on fraud detection as reported by the financial institutions personnel will accurately reflect the actual incidence and detection of fraud within the supervised institutions. The sample of financial institution officials surveyed is representative of the wider population of relevant experts within the Harare central business district financial service sector. The study will be successfully completed.

1.8 Delimitations of the Study

- i. The study is confined to financial institutions domiciled and operating within the Harare Central Business District. Harare, as the capital city, hosts the head offices and primary operations of most major banks and non-bank financial institutions, making it a suitable location for this study.
- ii. The study will focus on top tier financial institutions and low tier institutions because of limited resources.
- iii. The research will be conducted for period of close to 8 months from December 2025 to June 2026 having ample time to compile data and gather resources to perform the research.
- iv. The study captures data from those mainly involved in the internal control implementation, evaluation and monitoring. Excluding other parties which are not directly involved in this process.

1.9 Limitations of the Study

- i. Reluctance to disclose sensitive fraud data from control weakness, audit findings due to reputational risk and regulatory restrictions. To have progress from this hurdle the researcher provided a formal introductory letter from the university assuring confidentiality and academic use and use of code names pertaining the participant identification.
- ii. Social desirability and response bias, internal auditors might overstate the effectiveness of their control mechanisms to portray how good they are at the job. To clear the smoke the researcher collected data using self-administered questionnaires, in depth interviews with selected audit managers and a review of fraud detection reports.
- iii. Time and resource constraints thus what made the research only to select Harare central business district where most financial institution have their headquarters or major branches.
- iv. Generalizability beyond Harare central business district, findings may not be applicable to other cities due to transaction values and fraud patterns. the study was explicitly stated that conclusions are limited to Harare central business district.

1.10 Definition of terms

Fraud it is any premeditated or careful act to rob another of property, money by cunning, trickery or other discriminating means. The black law dictionary which defines 'it as a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment. ACFE, (2004).

Detection it is the systematic process of identifying or discovering the existence of abnormalities and behavioural indicators that may indicate the existence of wrong doing within an environment. That diverge from the established norms of operation.

Internal control is a procedure carried out by the board of directors, management, and other staff members of an organization intended to offer a reasonable level of assurance regarding the accomplishment of goals pertaining to operations, reporting and compliance. (COSO, 2013).

1.11 Summary

This chapter has introduced the critical problem of financial fraud in Zimbabwe and positioned the effectiveness of internal controls as a key variable in addressing it. The background highlighted the persistent challenge of fraud despite the existence of regulatory frameworks and the COSO-based control systems. The statement of the problem formally identified the gap between the theoretical promise of internal controls and their practical failure to adequately unearth fraud, leading to the study's purpose: to examine the relationship between internal control effectiveness (and fraud detection. Specific research questions were formulated to guide the inquiry. The significance of the study was articulated for regulators, financial institutions, and scholars, while the assumptions, delimitations, and limitations clarified the scope and constraints of the research. The subsequent chapters will present a comprehensive review of related literature (Chapter 2), detail the research methodology (Chapter 3), present the analysis of findings (Chapter 4), and offer a discussion, conclusions, and recommendations (Chapter 5).

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This chapter critically reviews the literature used to determine the effectiveness of internal controls in unearthing fraud within financial institutions, with a particular focus on the Zimbabwean, Harare (CBD) context. The review is structured to provide a comprehensive theoretical and empirical foundation for the study. Fraud diamond theory, control fraud theory and the theory of collusion. Fraud Triangle Theory, which remains the dominant explanatory model for fraudulent behaviour in organizational settings. Following the theoretical exposition the chapter presents a detailed synthesis of past empirical studies, The chapter concludes by identifying the research gap that this study aims to address, summarizing the key themes and stating the conceptual framework that will guide the empirical investigation.

2.1 Conceptual Framework

2.1.1 Internal controls

Internal controls are procedures carried out by directors and management to create logical assurance regarding the achievement of goals in three forms which are as follows operational effectiveness and efficiency, financial reporting reliability and legal and regulatory compliance. COSO, (1992). They are also a distinction between administrative controls and accounting controls. Administrative controls safeguard operational effectiveness and adherence to rules and procedures, whereas accounting controls are safety measures to manage assets and guarantee the accuracy of financial records. COSO, (1998). Any discussion of fraud detection and prevention must start with the idea of internal control because they are designed to provide reasonable assurance in achieving company objectives while preventing fraud and detecting errors. They are

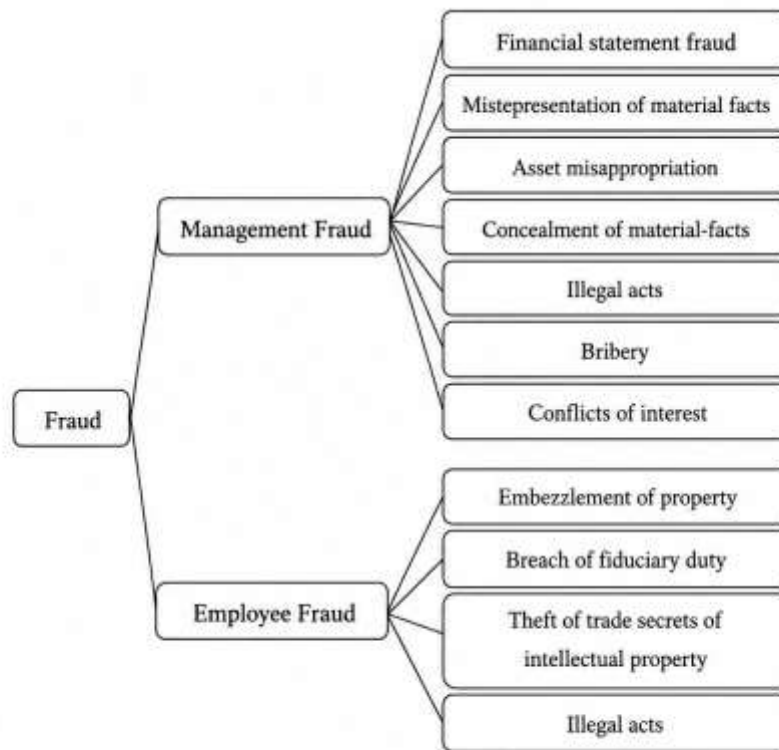
also implemented in different forms which might include segregation of duties, the use of passwords, authorization and approval, physical security and documentation policy.

2.1.2 Fraud

It's nearly impossible for criminologists and lawyers to agree on a single definition of fraud because it has many different forms, patterns and executions. This is because the Latin word "fraus" has many different meanings (Lavanti 2001). Fraud has four parts which are false representation of a factual nature, knowing that the representation is false or reckless disregard of the truth, relevance (meaning that the person receiving the presentation can reasonably and justifiably rely on it) and damage (meaning the money is lost because of the above). Skelah et al. (2003). In another context fraud is an economic crime that involves falsification of information, facts by perpetrators who possess the power to stand between officials and public, looking for an isolated gain. Murphy et al. (2009). It can also be viewed as an act of purposely hiding the truth from someone in order to encourage the targeted person to fall to the plot. Garner (2004). Furthermore, fraud can also be regarded as being dishonest with the objective of having an advantage for yourself or some third parties, avoiding responsibility and causing loss to another party, it is also underscored by the Anti-Fraud Policy, (2008). Crimes such as deception, forgery, extortion, corruption, theft, embezzlement, asset misappropriation, false representation, concealment of substantial facts, collusion, conspiracy and bribery fall under the fraud umbrella.

From the above meanings it can be seen that fraud is anything that is designed to mislead, an act of deceit for a personal gain and it is dedicated by the management, employees and third parties. Fraud is divided into management and employee fraud, as they perform their daily duties, they also come across loopholes which sometimes manipulate and cover up using their positions. Razaee (2001).

Fig 2.1 Classification of fraud activities



Source: Razaee (2002)

From the evaluation it is evident that financial statement fraud is contained within management fraud rather than employee fraud. Financial statement fraud is usually committed by managers particularly because it under their purview. Razaee (2002). Management fraud in another view is when the management conduct financial data manipulation of certain transaction in order to conceal their fraudulent acts. Brewer and List, (2004) .It is a fairly rare scenario because of their position to safeguard the organisation assets, however when it happens it acts like a time bomb you never knew was own because it will drag the shareholders' value down and reward the fraudsters scrapping a larger percentage of the profitability of the financial institutions .The lower level but hard to notice is employee fraud which can be best described as deceitful acts conducted by an worker of an organization for a personal gain at the expense of the company for example payment fraud, assets misappropriations and receipts fraud. (Garner, 2004). Some core internal malpractices which are faced by organizations are as follows,

- Theft and embezzlement. It involves the conversion of organizations assets and convert them for personal use. This can include an accountant using the petty cash to finance their own life expenses. Even receipt manipulation which will produce a lesser total revenue balance than the one which would have been received.
- Falsifying an organization's financial records to make it appear more or less lucrative is known as fraudulent statements. This can involve recording expenses over an extended period of time or booking phony sales (Fair 2007).
- Inventory: Any plan that involves stealing or misusing tangible, non-cash assets like supplies, equipment, or inventory. A worker pilfers goods from the sales floor or warehouse. Incoming merchandise shipments are diverted by an employee for personal purposes (Fair 2007).

When hiring new employee's management must conduct background research, confirm their referrals and certifications about the person of concern to eradicate the occurrence of fraudsters. It is essential that owners and managers clearly communicate organizational policies and procedures, such as codes of ethics to their staff. Henry, (2016) and shallow hiring policies can create conditions in which occupational fraud is more likely to occur. (Peltier-Rivest & Lanoue, 2015). Additionally, during employee training management should draw line on the importance of understanding anti-fraud measures to reduce cases of fraud. The management should also implement tailor made fraud-related training based on employee job responsibilities could enhance its effectiveness (Gates, Prachyl, & Sullivan, 2016; Peltier-Rivest & Lanoue, 2015). Staff which is properly exposed to the fraud threats that they will likely face in their respective workstations are always alert and proactive to fraud incidents (Henry, 2016).

2.1.3 COSO framework

It poses the most authoritative and widely adopted framework globally, originally released in 1992 and updated in 2013, the COSO framework provides a comprehensive model for designing, implementing and evaluating internal control systems. It is a benchmark for financial institutions which operate under intense regulatory scrutiny and face complex risks including financial data protection, anti-money laundering fraud prevention and operational resilience. The framework divided the internal controls into 5 components which are as follows;

2.1.3.1 Control Environment

It is the egg shell for all other components containing integrity, ethics and competence of the organization's people. It includes the way in which the organisation is directed and the way authority and responsibility are assigned. COSO (2013) A strong control environment draws the line at the top and it is crucial on fostering ethical culture of compliance and fraud awareness. It establishes the culture and values set by top management. The control environment establishes the attitude of the organization by persuading the control alertness and adherence of the staff. Whittington (2001) The factors include integrity and ethical values of employees responsible for creating, directing and monitoring controls, commitment and competency of employees carrying out assigned duties, or audit committee, management values and operating style and organizational structure.

2.1.3.2 Control Activities

Policies and plans are set in a specific organization to manage fraud and also the risk of human errors. They include events such as reconciliations, authorizations, verifications, assessments of operative performance and separation of duties (Whittington 2008). These controls affect the entire organization and all functions in specific departments. Control directives contain a range of significant roles in the control environment. Horngren (2012) such as,'

- To reduce the risk of asset loss or mismanagement, certain control measures are set. These include creating passwords to prevent unwanted access, physically storing tangible and intangible assets, backing up computer records and programs, conducting sporadic verifications of the quantity and condition of assets and creating facilities that are not on-site.
- Segregation of duties various staff members are assigned with approving transactions, documenting and keeping asset custody. It makes it challenging for an employee to make mistakes in the regular course of his work and cover them. Eradicating the asset misappropriation.
- Approval, verification and reconciliation, an employee is given permission by management to carry out specific tasks and complete specific transactions within set parameters. In addition, management lays down those duties or transactions that need

supervisory authorization before they are carried out by employees. A supervisor's approval indicates that the employee is verified and validated that the activity conforms to established policies and procedures. It shows the organization has a playbook in which it follows.

2.1.3.3 Risk Assessment

This involves the dynamic and iterative process for finding and evaluating risks to attain the organization's objectives for financial institutions it is fraud risk. It requires highlighting objectives, identifying internal and external risks considering the occurrence of fraud and determining how risks should be managed. Risks can come from many places, including changes in the operating environment, new personnel or new information systems. An efficient control system allows management to manage major risks and keep an eye on the accuracy and dependability of financial data disclosed to the public. Cingram, (2007),

- In order to identify risks management evaluates the entire business and determines which sections are most likely exposed to fraud, non-compliance and errors. To address recognized risks management develops appropriate controls.
- In risk management the management assesses the likelihood that a certain risk may materialize and result in monetary loss or non-compliance with the organization's regulations. The organization must decide whether to accept the risk and reduce it once it has been detected. Management evaluates risks by being directly involved in the day-to-day activities of the client community association and by being aware of the environment in which it functions Thompson (2001). Employee mistakes, omissions and delays are the main types of risk. Risks include poorly safeguarded assets, breaking rules, regulations and producing untrustworthy reports.
- Risk assessments are an ongoing process of discovering, assessing, and managing risk. Internal Control and Audit Tracking Policies (2010). A plan for identifying both internal and external risk is necessary for management. It is possible for management to comprehend how those risks impact their operations, assess their consequences, control their operations, mitigate their adverse effects and conduct continuous monitoring.

2.1.3.4 Information and Communication

This component ensures that relevant, quality information is identified, captured and communicated in a form and timeframe that enables people to carry out their internal control responsibilities. Effective communication must occur internally throughout the organization and externally (with stakeholders, regulators, and customers). Reliable information should be disseminated throughout the organization in an episodic fashion regarding its plans, risk, control environment, activities and performance (Horngren et al. 2012). Systems for information and communication comprise of;

- Inscribed policies and measures
- Mission statements
- Organizational charts
- Job descriptions
- Training material
- Periodic reports evaluating the organization's progress towards achieving its goals and objectives
- Internal and external reports

Financial reports Information and communication help employees comprehend the organization's objectives and it gives management reports that include operational, financial and compliance data so they can evaluate how well the goals are being met and take corrective action.

2.1.3.5 Monitoring Activities

These are ongoing appraisals, separate assessments or a combination used to establish whether each component of internal control is present and functioning. Monitoring involves assessing the quality of internal control performance over time and taking corrective actions if they are a need. In the financial services sector, the COSO framework provides controls organized across these five domains that can be mapped to specific governing requirements, helping institutions avoid compliance gaps and reduce the load of managing overlapping obligations from multiple regulators. The framework is considered a valuable function for fraud detection, especially in the

modern era characterized by complex financial products, digital transactions and stringent regulatory requirements. Monitoring as the assessment of internal control performance over a stretched period of time. Jones, (2008). These activities are related to the whole organization affecting all levels and functions. Internal controls are perceived to be properly designed and maintained if all the five mechanisms are existing and operational (Hornngren et al. 2012). Internal controls are effective if the management and stakeholders are guaranteed that:

- Organizational objectives are being attained
- Financial operations are producing dependable statements
- Compliance with laws and regulations

The COSO framework can be summarized graphically as shown below.



Figure 2.2 COSO Framework

Source: COSO 2013

2.2 Theoretical Framework

To understand why fraud occurs and how internal controls can solve it, it is essential to anchor the study in robust criminological and organizational theories. The most foundational is the Fraud Triangle Theory.

2.2.1 The Fraud Triangle Theory (Cressey, 1953)

Donald Cressey 's seminal work, "Other People 's Money "(1953), posits that three conditions must be present for an ordinary, trusted person to commit fraud perceived pressure or incentive,

perceived opportunity and rationalization. The model serves as a qualitative lens through which to evaluate and interpret potential fraud risks within an organization.



Figure 2.3 The fraud triangle

Source: ACFE The first element of the fraud triangle is perceived pressure.

2.2.1.1 Pressure

Pressure is a motivation to a person committing fraud. Pressure is in two forms financial for example (personal debt, lifestyle expectations) or non-financial (pressure to meet unrealistic performance targets). In a corporate setting, pressure to show inflated profits to trigger bonuses is a classic example. Lister (2007), characterized the pressure for one to indulge in fraudulent activities as "the prime basis of the heat for the fire". This suggests that experiencing this pressure does not automatically lead to deception. Rae and Subramanian (2008) supported the notion that financial pressure and greed on the part of the employee is a factor in the incentive to commit fraud. Chen and Elder (2007) identified six fundamental areas for pressure a violation of a commitment, personal issues, corporate invasion, status, achievement and interaction among workers. According to Abdullahi and Mansor's (2015) discussion of Chen and Elder's (2007) research, pressure can be divided into four categories as identified by Albrecht et al. (2008), all of these categories are relevant to the financial service sector. These categories include economic pressure, pressure related to vices, pressure related to one's job and other forms of pressure. Singleton et al. (2006) revealed that these pressures are often the baby steps in the process of committing fraud. However, it's essential to note that this financial pressure could be symptomatic of other underlying issues that the cheat may be facing. As such, it is crucial to take a complete

approach when identifying the root causes of fraudulent behaviour. Financial pressure or incentives can lead employees or management to commit fraud, such as accepting bribes in financial service procurement. Kenyon and Tilton (2006)

2.2.1.2 Opportunity

This is the element that internal controls are designed to eliminate. Opportunity arises from weak internal controls, poor management oversight, inadequate segregation of duties or the ability to override existing controls. The Fraud Triangle explicitly identifies weak internal controls as the factor that allows the fraud to occur. No matter the intensity of pressure, fraud cannot happen unless an opportunity is there. Hooper et al. in Abdullahi and Mansor (2015), According to Abdullahi and Mansor (2015), The opportunity goes hand in hand with pressure or motive since even if a person has a purpose, he cannot conduct fraud if a chance is not present. The weaknesses of controls, low work supervision and no clear segregation of duties on employees will create opportunity for fraud to occur. Employees who engage into fraud survive long years of service because they want to continue exploiting the loopholes and continue cover their previous acts which can be done whilst you are still employed. The ACFE, (2004)

2.2.1.3 Rationalization

This is the psychological component where the fraudster justifies their actions. Common excuses include “I am only borrowing the money”, “Everyone does it”, or “I deserve this because I am underpaid”. While difficult to control directly, a strong ethical culture and robust control environment can discourage rationalization. Reasoning is used as a backend defence mechanism by perpetrators in a way to give them assurance that the crime is doable. Rae and Subramanian (2008). As a result, it is argued that person without a good rationalisation statement is unlikely to commit the crime. Hooper and Pornelli (2010). Classical criminologist (Cesare Beccaria), (1764) argued that criminal action is triggered as a result of free and rational decisions of acting individuals (Hedonism) that is we seek pleasure and avoid pain. Another theorist who supported the idea of rationalization (J. Bentham) who ascertained that hedonistic calculus individuals are assumed to logically weigh the benefits of a given course of action against its costs. The Fraud Triangle remains the dominant framework. Auditors often use it for fraud prevention and detection and it has been adopted into professional standards including the American Institute of Certified

Public Accountants Statement on Auditing Standards (SAS) No. 99, which explicitly requires auditors to consider these three risk factors when assessing fraud risk.

2.2.2 Fraud diamond theory

The fraud diamond was established in 2004 as an extension of the fraud triangle (Wolfe and Herman, (2004) without the element of capability which makes up the fraud diamond theory. Without the capability to exploit the shortcomings of control it may be impossible to commit and hide fraud (Dorminey et al., 2012). Furthermore, in the context of the Fraud Triangle, capability increases the chance to construct by limiting the opportunity of those who have the necessary capability (Dorminey et al., 2012). Hence, Wolfe and Herman (2004) explain that for fraud to occur four elements of incentive, opportunity, rationalization and individual's capability must be present. This is represented graphically below.



Figure 2.4 The fraud diamond

Source: Wolfe and Hermanson (2004)

Therefore, Wolfe and Herman (2004) explain that the chance to commit fraud may occur in the presence of weak internal controls or oversight. However, without the person with the right capabilities to realize the opportunity and be able to exploit it, the act of fraud may never take place. They gave observable traits for committing fraud as

- The organization roles can provide the ability to create or exploit the opportunity to commit fraud.
- The perpetrator must be intelligent enough to understand and exploit the internal control weaknesses.
- The right person has a strong ego and great confidence.
- He or she must be a persuasive person in order to coerce others to conceal the act.
- The person must be able to stand by the first words and not bow down to guilt.

2.2.3 Control Fraud Theory

Control Fraud Theory is associated with criminology wheeler and Rothman (1982). Economics, Akerlof (1970), reviewed by William. K. black (2010) particularly relevant to institutional failures, such as the banking collapses examined in this study. It posits that fraud is committed by the CEO or other head of an organization who uses their position of control and perpetrate fraud against the stakeholders. In the context of state-owned banks in developing countries, control fraud has been linked to weak regulatory frameworks, political influence, lack of oversight by corporate regulatory bodies and personal collusion of bank personnel. According to Pindula,(1998) Zimbabwe financial service sector witnessed the closure of UMB due to fraud activities which destroyed the bank to shambles due to management inefficiencies. The override of control systems of the bank led to its demise the management became overboard of the control systems.

2.3.4 Theory of collusion

It is described as a deceitful agreement or secret cooperation between two or more parties limited to open competition by deceiving, misleading and defrauding others from the true cause. J.E. Harrington (2017), ACFE, (2022) gave a report on how companies suffer losses of more than 5% per year due to fraud. 58% of those cases are collusion showing the great impact of collusion to the overall financial performances. The internal control systems are basically designed to factor out errors. Criminals commit fraud in a coordinated approach to avoid detection. For instance, a low staff level working with high level management to commit fraud, the paper trail of the act might not be found in an auditing exercise even done properly because first entries will be scrapped

of the books. It goes undetected. This approach will make the crime be erased from each level of the organization. The systems are there but loopholes are being manipulated.

2.4 Empirical review

The following are some examples of empirical evidence that have been found in studies on the effectiveness of internal controls in detecting fraud in the financial service sector focusing on those based in Harare CBD.

Murti and Kurniawan (2020) carried out a study on the implementation and internal control in preventing fraud using in the public sector.

The study found out that the ineffective internal control measures are the main drivers of fraud. The issues of fraud cannot be eradicated fully but to solve it management must put in place robust measures to help reduce its menace in the organization's structures. Anti-fraud awareness trainings must be set in place in public institutions to increase the awareness of employees who are at the risk of encountering fraud. It will combat the employees with necessary tools to fight and prevent fraud.

Takavingofa (2017), embarked on a study of the effectiveness of internal control systems used by parastatals in Zimbabwe in reducing the risk of fraud.

The literature review used added that ineffective controls create breeding grounds for fraudulent activities in parastatals. The major finding of the research was that the internal controls measures used were not strong in the fight against fraud and advised the management must conduct a thorough clean up on their internal controls to strengthen them where they are failing to produce effective results. They should also take a risk assessment focused on the whole organisation in dealing with fraud.

Aduam (2015) to investigate the effectiveness of internal control measures implemented in the Techiman Municipal Assembly (TMA) in Ghana.

The study employed an illustrative case study research design and the data collected was analysed SPSS. External pressures and political interference were one of the main causes the organisation failed to operate according to the internal control manifest, system override was more visible in the study results. Most public officials are not fully liable to the action as service delivery is mixed

with political favours. To understand the reasons behind of first-party fraud in e-tailing, the authors used academic literature for the understanding the body of information on first-party fraud. The study highlighted a range of first party fraud methodologies implemented and the loopholes which promoted its occurrence. The designed control system was not adhered to leading to the organisation facing financial and administrative problems. Amasiatu and Shah (2014)

Mugari, Gona, Maunga, and Chiyambiro conducted a study in 2016 to identify prevalent types of cybercrime in Zimbabwe's financial sector and the effectiveness of existing countermeasures.

The study was on commercial banks in the Harare area and focused only on four of them. The main area of concern was hacking which attributed to 75% highlighted by the respondents. The banking institution posed their own precautionary controls measures which include education and training workshops and seminars, strict security measures, regular system updates, communication and technology, the installation and constant updating of security measures like anti-virus, firewalls, and data recovery sites. The banks were more prone to hacking, identity theft and harmful software usage. Recommendations were that the financial institutions had to include training, software upgrading and firewalls on their control measures playbook.

Okafor (2020) conducted the study on the factors affecting strategies of combating fraud.

The study used a mixed technique in the investigation processes. Senior employees, junior employees from various departments made up the study's target group. Data from respondents was gathered using a stratified random sampling technique. T tests, averages, percentages and frequencies were among the statistical tools utilized to examine the data. The study showed that the organogram of the organisation hindered the power of fraud prevention tactics.

Oronde (2022) conducted a descriptive and analytical study on the factors that hinder the effectiveness of strategies aimed at preventing fraud in Kenya.

The study used quantitative and qualitative methodologies. Qualitative involved interviews, observation and focus group discussions, while questionnaires were involved on the quantitative data sources. Document analysis was used on the secondary data. The study randomly selected 28 respondents from all of employees available. It was observed that weak internal controls, use of

authority to bypass existing internal controls and organizational structure complexity were the key metrics which hindered the prevention of fraud.

L.A.Mwonge (2022) the effectiveness of fraud prevention and detection methods in the public sector.

The study purpose was to validate the efficacy of fraud prevention and detection measures in Tanzania's public sector. The overall findings indicated that the most effective control processes were those involving internal controls review also implementing the improvements, cash reviews, inventory inspection and bank reconciliation. These were followed by staff communication, integrated fraud control, organizational policy continuous monitoring, inspection tools and methods and the protection software application, The study suggested that integrated fraud control, organizational policy, continuous monitoring, tools inspection and software application protection were ineffective, parastatals should improve by checking their performance scores.

Chintrakarn and Herzer (2010) conducted research in the United States to determine the effective strategies in preventing fraud.

The total population of the study was 1752, and a selected sample size of 337 was identified using the Borg and Gall (1973) sampling method. They implemented structured questionnaires as their research instruments, they were validated using a face content validity method also their reliability was conducted using test-retest and Cronbach's Alpha assessment. The data was valuated using simple percentages and descriptive statistics and Multiple Regression Analysis (MRA) at a 0.05 level of significance was used in testing the hypotheses. The study showed that preventing fraud using internal controls gave a positive reduction in fraud activities.

Cortes, Santamaria, and Vargas (2016) conducted a research study in India on the approaches used to minimize fraud.

The study utilized a descriptive research design and five research questions directed the study. To achieve their objectives the researchers added explanatory research designs adopting a mixed research approach. The population constituted employees from Cans BANK and 600 employees were selected from different departments. Expressive statistics such as mean and frequency tables, were employed to present the results. SPSS the analysis tool was used to determine correlations

and regressions among the variables. The study showed that creating a safe space for employees to share their views and violations is an effective way to the reporting of fraudulent activities helping combat fraud.

2.5 Research Gap analysis

Some studies focused on the application of internal controls in the public sector and its impacts. To provide results they used literature from various publications citing about internal controls of parastatals and public sector. The authors highlighted that poor internal controls systems were at the centre stage of promoting fraud due to corruption involvement. Murti and Kurniawan (2020). This research focuses on the internal controls as a way of detecting fraud in financial service sector focusing more on those domiciles in the central business district of Harare.

This research focused on efficacy of internal controls utilised by parastatals in Zimbabwe in reducing the risk of fraud. The study focused most prevalence types of frauds that affected the growth of parastatals also the most utilised control mechanism. Takavingofa (2017). The study sharpest angle was to evaluate the best control measures that can used to detect fraud in the financial service sector domicile in Harare CBD and the study also delved deep to point out the forms of financial fraud that hinder the success of any business.

Fraud remains a notable concern in the international financial sector, posing hazards to the firmness and proficiency of financial systems. The domestic financial sector is no exclusion, facing tenacious challenges related to fraud. Although there is current literature on internal controls and fraud in the financial service sector, studies precisely talking about the effectiveness of internal controls in detecting fraud within this context, particularly with a dedicated focus on financial service sector domicile in Harare central business district between 2025 and 2026, are limited. Furthermore, the recognized research gap highlights the urgency for the evaluation of the effectiveness of fraud detection (internal controls) measures rather than general discussions on fraud occurrences. The specific examination of those domicile in Harare CBD allows for a case study that provides insights into the effectiveness of fraud detection measures employed by the of Harare financial service sector.

2.6 Summary

The literature reviewed highlighted much research which was conducted before showing all relevant aspects of fraud from occurrence, combating and detection. Showing all forms of fraud and how best we can solve the mystery. The study main aim is to show how effective internal controls are they to detect fraud in financial service providers domicile in Harare CBD.

CHAPTER 3

RESEARCH METHODOLOGY

3.0 Introduction

This chapter outlines the methodological framework employed to investigate the effectiveness of internal controls in detecting fraud within the financial services sector. It provides a detailed interpretation of the research philosophy, approach, strategy, data collection methods and analytical techniques used to ensure the study's validity, reliability, and ethical integrity. By adopting a mixed-methods approach. The researcher aims to ensure a healthy framework to address the research objectives and fill the gaps identified in the literature review, particularly the research gap analysis.

3.1 Research design

Research design performs as a guide to the researcher in the course of gathering data, evaluating and rendering it (Keith et al, 2007). Coming up with a research design will give a thorough plan which will be utilized to direct and focus the research being carried out. Collis and Hussey (2009) Designing research supports the researcher in preparing and coming up with the study in a way that would enable the researcher to acquire anticipated outcomes, (Burns and Grove 2001). A case study is an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-world context. Yin, (2018). A single financial institution can serve as a benchmark case, offering unique access to its internal control processes and personnel. The significance of this methodological design is underscored by the unique contextual challenges facing Zimbabwe's financial sector, including economic volatility, currency instability and increasingly sophisticated fraud schemes. Chitimira, Torerai & Jana, (2024). Previous studies conducted in the Harare CBD have identified internal bank fraud as a significant issue, with fraud cases increasing by 205.9% between 2010 and 2011, highlighting systemic vulnerabilities in the banking sector. The methodology adopted herein draws from established frameworks in similar studies conducted in

Ghana, Nigeria, Kenya, and Palestine, while remaining sensitive to the local Zimbabwean regulatory environment governed by the Reserve Bank of Zimbabwe (RBZ) and the Money Laundering and Proceeds of Crime Act [Chapter 9:24].

This strategy allows for triangulation of data from multiple sources to build a rich, detailed picture.

The mixed-methods design involves two separate but complementary phases:

- Quantitative Phase: To establish a baseline of measurable effectiveness.
- Qualitative Phase: To explore the nuances, challenges and contextual factors behind the quantitative findings.

3.2 Target population

The target population for this study covered all registered financial institutions operational within Harare Central Business District including commercial banks, building societies, microfinance institutions, insurance companies and asset management firms regulated by the Reserve Bank of Zimbabwe and the Insurance and Pensions Commission (IPEC). The population involved employees assigned to the following departments internal controls and fraud risk management within these institutions, specifically: Internal auditors, Risk managers, Compliance officers, Fraud investigation officers and Senior finance managers. These contributors came to a total of 120 which were selected because of their direct involvement in designing, implementing, monitoring and evaluating of internal control systems and their expertise in fraud risk management (IRJMS, 2025). Harare CBD was selected as the geographical locus of the study because it represents the financial hub of Zimbabwe, hosting the headquarters and principal operational centres of the majority of the country's financial institutions. Previous research has acknowledged that Harare CBD financial sector as predominantly vulnerable to internal fraud due to high transaction volumes, complex organizational structures and the concentration of high-value financial activities.

3.3 Sampling

It is a process of selecting a portion of the portion of population to represent the entire population. Hungler, (1991). Sample can be defined as a group of people or subjects chosen out of larger number and asked questions in order to get information about a large group. Russel, (2001). A sample is a small part of population, which has the same characteristics of the population'. The

Reserve Bank of Zimbabwe's 2024 licensed financial institutions and the Zimbabwe Stock Exchange (ZSE) directory of listed financial services companies with operational headquarters in Harare CBD was used as a sampling frame. This frame ensured that only regulated and legally operating institutions were included to enhance the legitimacy and generalizability of findings within the formal financial sector.

3.3.1 Sampling Techniques

The study used purposive sampling as a non-probability sampling technique in which the researcher deliberately selects participants who have specific characteristics, relevant experience to the study and knowledge. John W. Creswell (2014). A combination of purposive and stratified random sampling techniques was employed. Purposive sampling was used to select financial institutions that met specific criteria:

- Operational presence in Harare CBD for at least five years,
- Documented internal control frameworks,
- RBZ compliance history indicating active fraud risk management programmes.

This non-probability method is in line with earlier research on internal controls in African banking sectors, (Ubesie, Ibezim & Mgbobi, 2023; Yakubu, Alhassan & Sumaila, 2017). It focused on organizations with verifiable control systems. Individual respondents were chosen using stratified random sampling within the chosen institutions Internal audit, Risk management, Compliance, Fraud investigation and Senior finance were the job functions which determined the strata. This stratification guaranteed representation across all control-related functions and prevented over-representation of any single department.

3.3.2 Sample size

The sample size was determined using Slovin's formula, consistent with recent Zimbabwean financial sector research (IRJMS, 2025):

$$n = \frac{N}{1 + Ne^2}$$

Where:

- n = sample size

- N = target population (estimated 120 key control personnel across identified institutions in Harare CBD)

- e = margin of error (0.5 at 95% confidence level)

$$n = \frac{120}{1 + 120(0.05)^2} = \frac{120}{1.3} \approx 92$$

The number of respondents was 92 out of the 120 previously selected as the sample. A minimum of 8 to 10 financial institutions was targeted to ensure institutional diversity, consistent with case study methodologies employed in Cameroonian MFI research (Abei, 2021) and Zimbabwean banking technology studies (BUSE, 2024).

3.4 Research instruments

There are numerous ways to get information such as focus groups, surveys, questionnaires, interviews and observations. Creswell (2014). A semi-structured interview guide was employed in the study to generate in depth accounts of internal control views, inefficiencies and financial consequences related to fraud detection, Yin (2018). Each question provided flexibility for follow up questions to examine developing topics.

3.4.1 Questionnaires

A questionnaire is described as a research tool that consists of a series of questions and additional prompts that can be used to gather data from respondents. A questionnaire is a technique for collecting data in which participants are asked to react in a predetermined order to a specific matching set of related questions. Saunders et al. (2003), Information was gathered using a standardized questionnaire, the data collection process was simple.

3.4.1.1 Advantages of Questionnaires

- Large amounts of data may be collected from a huge population in a limited period of time and in fairly cost-effective way.
- Can be carried out by the researcher or by any number of individuals with little impact on its accuracy and dependability.
- The outcomes of the questionnaires can usually be quickly and easily quantified by either a researcher or concluded by the use of software package.
- Can be assessed more scientifically and precisely than other methods of research.

- They will not include interview unfairness as the respondent will not be sharing his views face to face with the interviewer.
- They offer confidentiality thus giving respondents the guarantee of their privacy and concealment.

3.4.1.2 Disadvantages of Questionnaires

- Inadequate to understand as they don't capture some forms of information such as changes
- Subjective in the sense that people perceive each question differently and respond according to how they see it, thus what is "good" to one person may be "poor" to another.
- There is no guarantee that the person listed on the questionnaire actually filled it out; for instance, a busy management may assign the assignment to their subordinates to finish on their behalf.

3.4.2 Interviews

An interview is a conversation in which questions are posed and answered to. In a one-to-one discussion, one person assumes the position of the interviewer and the other, that of the interviewee. Webster (2023) The researcher's data collection involved semi-structured, face to face interviews conducted with the 29 selected institution depending on availability. The semi-structured arrangement allowed for flexibility to explore surprising insights while sustaining the focus on the research objectives (Creswell and Poth, 2018). Interviews were scheduled over a less busy day, to ensure quality transcription and reflection. Chief Audit Executives / Internal Audit Managers, to gain a strategic perspective on control design and technology adoption. IT Security and Forensic Data Analytics Specialists, to understand the technical proficiencies, limitations and implementation of tools like AI and continuous monitoring. Fraud Investigators, to understand how technology-generated alerts are actioned and investigated. Operational Staff in Control Functions (e.g., Compliance Officers), to understand the day-to-day reality of using and being monitored by these systems. External Auditors (with permission), to get an independent perspective on the control environment.

3.4.2.1 Advantages

- interviews provide detailed and meaningful insights into participants experiences, making them valuable for qualitative research. John w Creswell (2007)
- Suitable for complex and sensitive topics.

- Higher response rate.

3.4.2.2 Disadvantages

- interviews are effective but they require considerable time and resources. Robert k. Yin (2003).
- Interviewer bias.

3.4.3 Justification

One type of primary data collection method is Interviews. Interview are dialogs in which questions are put by one person and responses given by another or a similar conversation in which one person ask questions and other responds or a similar exchange in which the interviewee shares information or opinions, usually more free-flowing manner than in a formal interrogation. They employ face to face interactions, telephone interviews and video conferencing. In person interactions will be conducted by the researcher. The researcher made use of them due to their ability to capture rich, environment-specific insights into challenging events such as internal controls identifying fraud. Qualitative interviews facilitated examination of stakeholder's particular experiences, perceptions and views on inefficiencies and financial impacts, which quantitative methods may overlook. (Yin, 2018). Semi-structured interviews balance structure and flexibility, enabling the researcher to address the 10 interview questions while tracking emerging themes, as supported by Creswell and Poth (2018).

3.4.4 Document Analysis

Shallow inspection, reading and interpretation are followed by document analysis There is a method of qualitative approach in which documents are analysed by researcher to provide expression and significance about the research study. (Bowen, 2009). Document analysis involve both the topic and content analysis. Publicly available bank financial statement, journals content, government publications are the materials examined in this study. Bowen, (2009). Internal Audit Reports (anonymized), to comprehend the kinds of results reported and the kinds of results reported and the controls that are formally tested. Fraud Incident Reports, to evaluate prior frauds and understand how they were (or were not) identified by the control system. Manuals policies and procedures to comprehend the control environments intended design. Reports produced by data analytics or monitoring are examples of system output reports,

3.5 Sources of Data

3.5.1 Primary Data

Primary data is data that is collected for the initial time and therefore is in the original state (Creswell, 2014). Primary data comes from first hand observation and experience. Kadam (2023). The study relied on primary data from semi-structured interviews with the 29 stakeholders, providing real time insights into the internal control systems of the targeted stakeholder in the Harare financial service sector.

3.5.2 Secondary Data

Secondary data is data that has been collected and analysed before used for a different purpose, and is then used for another study question (Creswell, 2014). To triangulate findings and enhance credibility, the researcher collected secondary data from banks, insurers, asset management, microfinance and money transfer annual reports, journal articles (published and unpublished), newspapers, and World Bank reports. Primary data offered stakeholder perspectives, while secondary data gave context to the findings, aligning with Saunders et al. (2019). For example, the financial annual report provides revenue and cost data to compare with interview narratives on financial viability. Secondary data information was studied, extracted and used descriptively to support the case study, as recommended by Saunders et al. (2019).

3.5.2.1 The Internet

Journals and eBooks journals are examples of online data that are useful for research. Numerous journals and eBooks that are helpful for research can be found on the internet. The internet is easy to use and gives the researcher access to all references. Questionnaires can also be sent via email thanks to the internet. Information about how other financial institution in other nations handle fraud cases and strategies for preventing them can also be found online.

3.5.2.2 Textbooks

The researcher used various text books and journals in relation to internal controls and fraud. The key advantage of using published books is that they are relatively cheap and extensively accessible since they can be borrowed from the University library free of charge.

3.5.2.3 Research Papers and Journals

These are known as data from earlier researches on the same focus or issue and were retrieved from publications and preceding presentations by global legendary authors and researchers. These groups have past performances on the issue they covered through seminars presented.

3.5.2.4 Newspapers

Newspapers were used in this study, as they provided an in depth of the existing issues in Zimbabwe in relation to fraudulent cases taking place in the country. The researcher collected information from the Herald, Chronicles and Newsday.

3.6 Data collection procedure

The researcher went to the Head Offices of targeted firms operating in the Harare central business district to inform the entity about the research. The Human Resource departments assisted the researcher to get a slot for interviewing the researcher's targeted population. During the interviews, the researcher took notes from the respondents because they refused to be recorded. The researcher got informed consent from all interviewees, coded the respondents as F1, F02, and F03 for confidentiality. The researcher chose respondents with expertise in financial operations like managers. With only 15 interviews, the researcher aimed for quality over quantity. Some responses were vague, so the researcher used follow up prompts to clarify ratings which was time consuming but worth it.

3.7 Data Presentation and Analysis

Data collected for interviews questions for the study was evaluated using thematic analysis, a qualitative method to point out, analyse and outline patterns known as themes within the interview notes. The researcher presented data in narrative form with tables summarizing themes and illustrative quotes from certain participants, ensuring clarity (Saunders et al., 2019). For example, a table listed themes like "participation" with quotes from like F01 stated this. Data collected for the study was presented in tables, pie charts and also an atlas ti software was used in coding interview responses.

3.8 Validity and Reliability

Validity refers to the scope to which an analysis tool measures what it is intended to measure. Creswell, (2014). Validity was attained by reviewing prior studies of the effectiveness of internal controls in unearthing fraud in the financial services sector. To ensure integrity, the study employed

triangulation, combining interview data with secondary sources as purported Creswell and Poth, 2018). The researcher also shared the interview guide with participants to verify accuracy, enhancing trustworthiness (Yin, 2018).

Reliability refers to the point analysis tools applied on repeated basis produce constant results consistently. The researcher employed a test-retest reliability whereby the same interview questions are asked to the same participants at different times. The higher the correlation between the answers at two sets of time, the higher the test-retest reliability. The researcher observed that the frequency of getting same responses was high with a frequency of 80% the same, therefore the responses given are reliable for the researcher to carry out their study.

3.9 Ethical Considerations

The study was conducted adhering to ethical principles to protect participants and ensure integrity, using the views of Saunders et al. (2019). The confidential and privacy of the respondents was respected and all data was coded. Data collected was used for this study's purpose only. Right to withdraw, participants will be informed of their right to withdraw from the study at any time without providing a reason. Minimizing harm, the topic is sensitive. Questions will be framed carefully to avoid causing professional or personal distress.

3.10 Summary

The chapter focused on analysis approach, taking into consideration the methods for gathering data, the population, research instruments used and the sample size based on sampling applicable. This methodology provides a robust and coherent plan to investigate the research problem. By combining a qualitative exploration of lived experiences with a quantitative measure of perceptions and by grounding the study in a real-world organizational context. The research is well-positioned to generate rich, credible and insightful findings that directly address the critical gap

CHAPTER 4

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

The chapter is arranged into data presentation, thematic analysis process, emerging themes, and discussion of findings, with tables and quotes ensuring clarity and accuracy using the views of Creswell and Poth, (2018). The information collected by the researcher will be presented in line with the research objectives which are forms of fraud, ways of combating fraud and factors affecting the effectiveness of combating fraud at the organizations selected. The findings made by the researcher will also be discussed.

4.1 Response analysis

4.1.1 Questionnaire response rate

92 questionnaires were distributed to the targeted population and the researcher managed to receive 59 completed questionnaires. This resulted in an overall response rate of 65 %. A non-response percentage of 35% was attributed to the targeted respondent's reluctance due to their busy schedules. Despite this, the researcher considered the 65% response rate satisfactory given the limited time frame for the study. A questionnaire response rate of 60% or higher is considered good source for research. Johnson, (2012). It valuated that the obtained response rate was well above the acceptable threshold. This high response rate of 65% positively impacts the reliability of the findings indicating that the information provided is likely to be dependable.

Response rate for questionnaire

Table 4.1

QUESTIONNAIRE	FREQUENCY	PERCENTAGE
RESPONDED	59	65
NOT RESPONDED	33	35
OVERALL QUESTIONNAIRE RESPONDED	59	65

Source: research data (2026)

From the table above shows that the response rate was 65% and it clearly shows that the majority of the targeted participants took part in the study. This response rate is generally considered adequate for research purposes because it provides sufficient data for analysis and reduces the likelihood of non-response bias. Therefore, findings obtained be regarded as reasonably reliable and representative of the study population.

4.1.2 Response rate for interviews

Table 4.2

Interviews	Issued	Success	Failure
Respondents	15	12	3
Percentage%	100	80	20

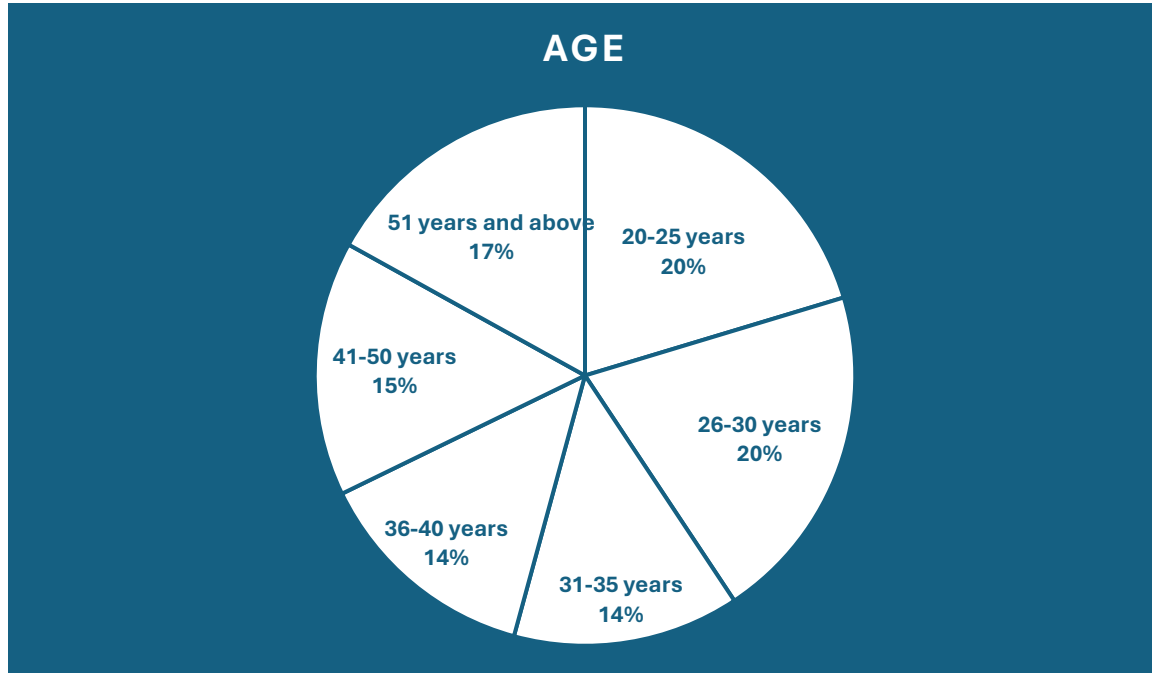
Source: research data. (2026)

From the table above the main aim was to interview 15 respondents, unfortunately only 12 respondents were interviewed. This meant that 80% was success rate for interviews conducted while 3 respondents failed to show up for interviews due to that they were assigned to attend business emergency meeting on the day of interviews. The data that was gathered through interview was used to complement the data that was gathered from questionnaires.

4.2 Quantitative analysis

4.2.1 Age of respondents

Figure 4.1

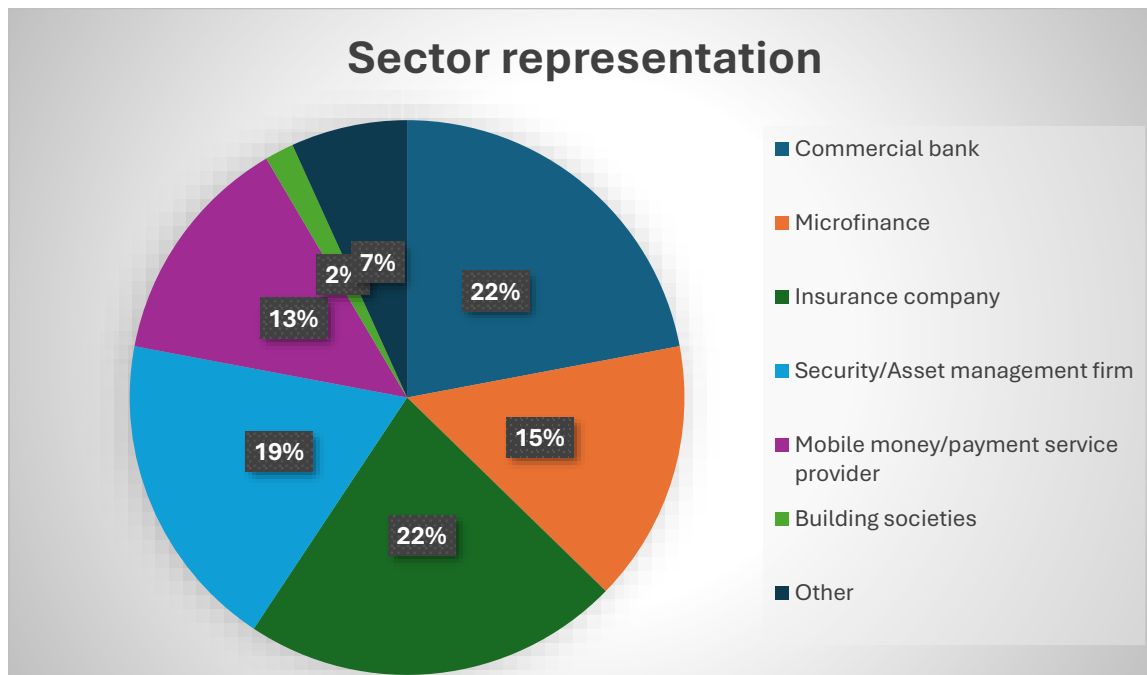


Source: Research data (2026)

The demographic sphere of questionnaire response was highly on the age range of 20-25 years, followed by 26-30 years and lastly 51 years and above. This showed that almost all age groups were represented by those who managed to respond. The sample relatively young, it reflects the broader employment structure in Zimbabwe financial service sector where the middle and lower ranks are more likely to complete surveys. The young employees may have different perceptions of internal control but also potentially less experience in detecting sophisticated fraud.

4.2.2 Sector participation

Figure 4.2

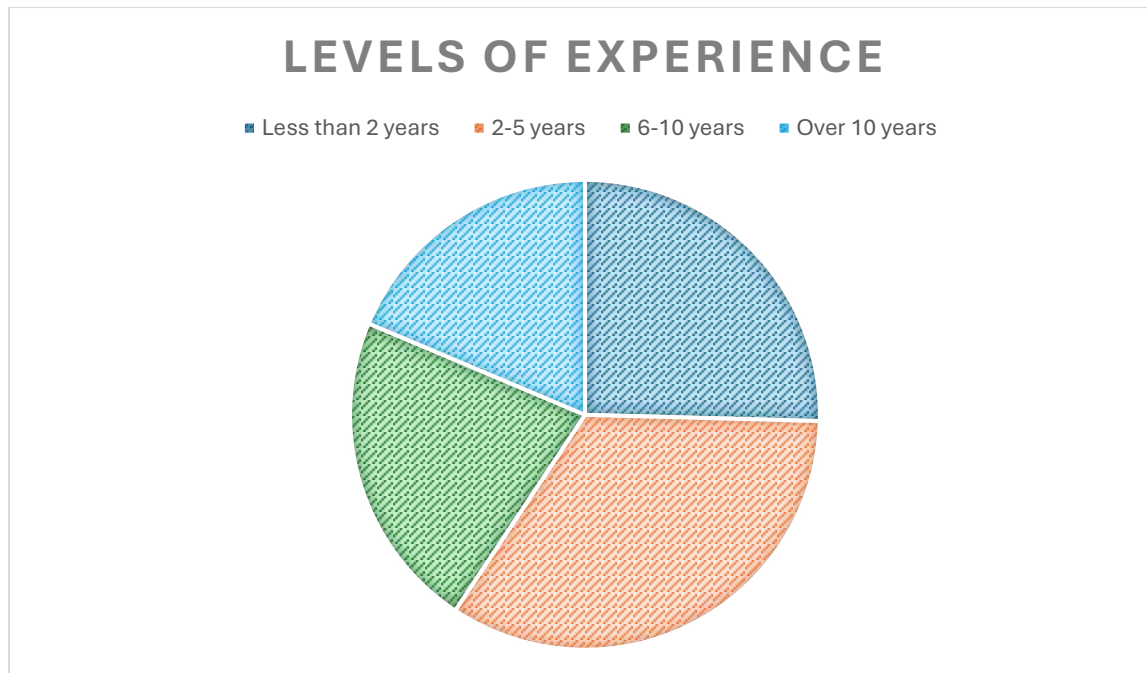


Source: Research data (2026)

From the questionnaires given out commercial banks and securities/asset management firms were highly responsive to this study. Commercial banks represent a higher value transaction in the financial sector and also insurance firms. They carry a huge percentage in the financial service market translating to the impact of their views on the outcome of these study. It is beneficial because they face greater fraud risk offering a comparative perspective. Similar sectoral weighting was used by KPMG (2018), in their fraud survey of East African financial institutions, where banks formed the core sample.

4.2.3 Level of experience

Figure 4.3



Source: Research data (2026)

The respondents showed a prevalent year range of experience of 2-5 years. Followed by a range of less than 2 years, followed by 6-10 years and over 10 years. This variation of experience levels is attributed to the more use of software's which made some workers redundant and also the organizational organograms which is thin at the top and broad at the bottom. Most respondents have moderate experience, meaning they understand daily control but may lack strategic oversight. Their views on the effectiveness of internal controls are grounded in operational reality not just policy.

4.2.4 Organizational departments.

Figure 4.4

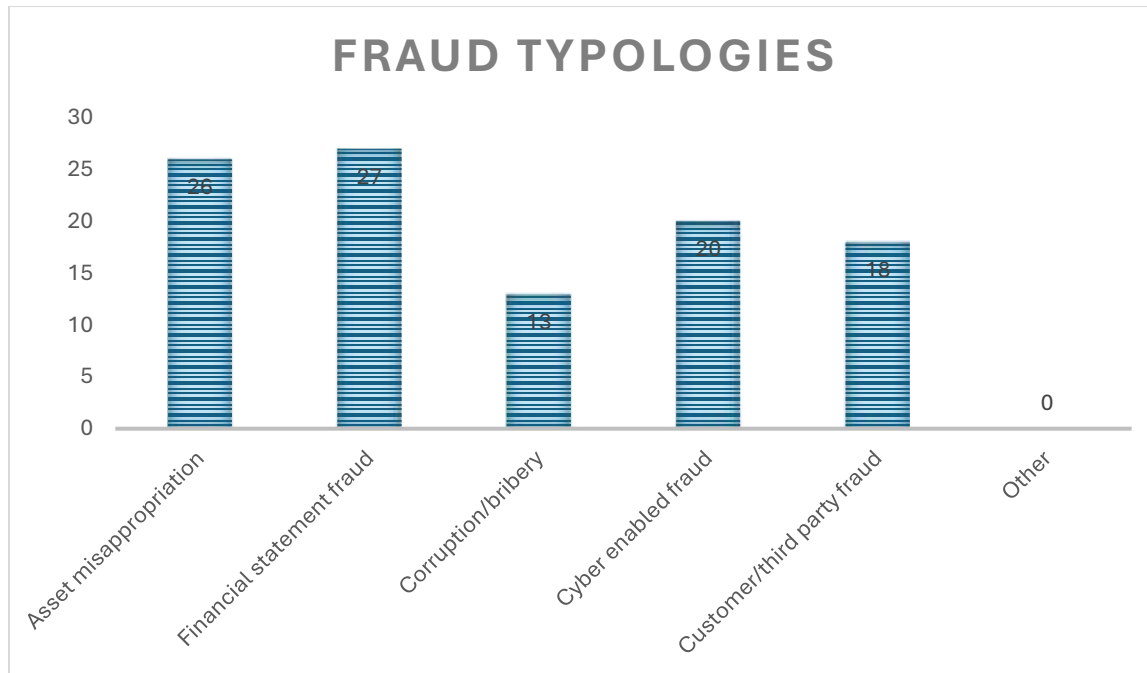


Source: Research data (2026)

The results showed the much participants of oversight roles which are internal audit, compliance, fraud investigation and senior finance officers. These are the people who draw lines, check the effectiveness of the lines and provide solutions to fix the issues. Oversight and control functions are heavily represented. This is because the selected personnel directly design, test or enforce internal controls. Their responses are more authoritative than those from frontline staff. Internal control assessments should involve those in control roles to give the authoritative view of handling the systems operations. COSO internal control framework. (2013)

4.2.5 Fraud typologies

Figure 4.5



Source: Research data (2026)

The forms of fraud commonly found in this sector are corruption or bribery, cyber enabled fraud, customer third party fraud, financial statement fraud and asset misappropriation. However, the researcher found out that asset misappropriation and financial statement fraud were more threatening to the financial service sector in the Harare central business district followed by cyber enabled fraud. The findings made by the researcher are similar with those made by, Joseph T Wells (2005) in United states he found out that the most common type of fraud typology was asset misappropriation this study supports the patterns currently occurring in Harare financial sector. Asset misappropriation accounts for 86% of all fraud cases but the lowest median loss, it has a high occurrence rate but its impact is on the mid-level compare to others. ACFE, (2022). Financial statement fraud although rare causes the greatest impact to financial institutions profitability. Cyber enabled fraud is a rising phenomenon in Zimbabwe (Harare CBD) because of the growing digital financial world.

4.2.6 Corporate environment in relation to internal controls

Table 4.3

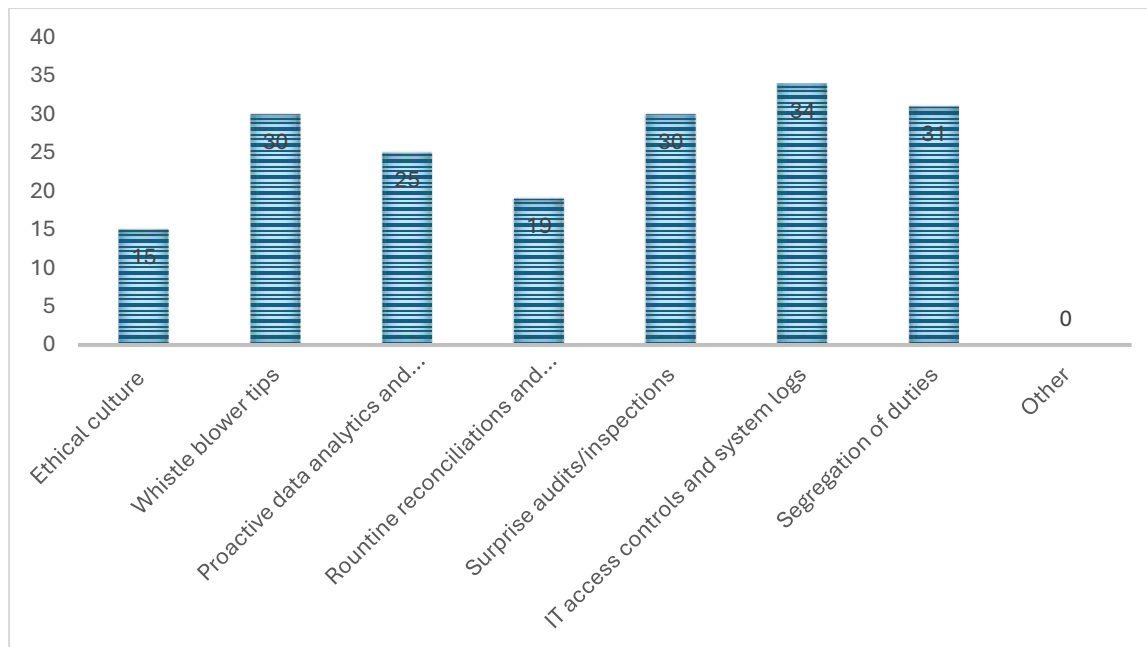
Corporate environment internal controls	Frequency
Management override of controls	29
Inadequate staff training on fraud awareness	35
Insufficient technological tools / data analytics	42
Collusion among employees or with third parties	34
Low prioritization of fraud risk by senior management	22
Understaffed or under resourced internal audit /compliance departments	20
Poorly designed or outdated control procedures	29
Lack of independence of control functions	19
Other	0

Source: Research data (2026)

The agenda of this objective is to have an idea on the corporate environment in relation to the internal controls of their organization to detect fraud. The more prevalent issue was the one of insufficient technological tools or data analytics to uncover fraud, followed by inadequate staff training on fraud awareness. The fraud ecosystem continues to evolve day by day what you studied 3 years back might not be effective today. Harare financial ecosystem recognize that fraud detection is hindered by outdated tools and lack of continuous training. Deloitte, (2020), produced an evaluation report on African banks that they often lag in adopting AI-driven transaction monitoring, creating a skills and tools gap. The findings of this study highlighted the same elements as loopholes to the occurrence of fraud.

4.2.7 The effectiveness of internal controls

Figure 4.6



Source: Research data (2026)

The purpose of the question was to see which internal control system used by the organization have been most effective in achieving their intended objectives, particularly the detection of fraud. The findings indicate that IT access controls and systems took a major score followed by segregation of duties which derails the problem of collusion within the employees. Corporate ethics failed to benchmark the strong position of these different organizations within the financial service sector against fraud highlighting the issues of management override against the controls system blueprint. Technical controls are viewed as effective, however corporate ethics the tone at the top is least effective. Weak internal controls, use of authority to bypass existing internal controls and organizational structure complexity were critical obstacles to the effectiveness of strategies aimed at preventing fraud. Oronde, (2022). Some past study's obtained results showing that complexity of the organizational structure affect strategies used in combating fraud. Okafor, (2020).

4.3 Qualitative data analysis

The interview question was divided into 4 categories derived from the main objectives of this study. The purpose was to try and see another view of participants on the internal controls used by these financial services providers. they are as follows

4.3.1 Internal Controls Currently in Place

“We have firm segregation of duties; the front office cannot handle settlement and reconciliation; it is conducted by a completely separate team. That is our first wall.” (F3, Internal Audit Manager)

“For digital system onboarding, we rely on a third-party KYC system. I’m not fully comfortable, but our core banking controls are strong biometrics, role-based access, and mandatory leave for cash handlers.” (F7, Compliance Officer)

“Surprise audits exercises happen at least once a quarter. But surprise is relative senior management sometimes gets a hint.” (F9, Fraud Investigator)

Respondents consistently point to a coated control framework. Preventive measures which are strict segregation of duties between front-office, settlement and reconciliation teams. A multi-level transaction approval limits, biometric and role-based system access and mandatory vacation policies for sensitive roles. Detective controls include daily automated reconciliation of nostro accounts, exception reporting for high-value or unusual transactions and periodic surprise audits by internal audit. However, many acknowledge that controls are strongest in traditional banking operations (cash handling, lending) and thinner in newer digital channels, where onboarding and transaction monitoring may rely more heavily on third-party systems. The financial institutions often face challenges in applying and monitoring controls associated with external systems and regulatory compliance requirements, some of them are not tailor made to the organisation work plan. Pinho, (2015). The study also noted that rapid digital transformation can create control gaps if oversight mechanisms do not evolve at the same pace.

4.3.2 Effectiveness of the current implemented internal controls

“Our transaction monitoring catches about 70% of known fraud patterns. But new schemes especially social engineering they slip through. No system is 100%.” (F1, Senior Finance Officer)

“We value ourselves to industry benchmarks through the Bankers’ Association. On paper we are average. But I’ve seen management override twice in three years that scares me.” (F5, Internal Audit)

“Effectiveness is uneven. Cash handling very high. Mobile banking fraud low. We are always one step behind.” (F11, Compliance Analyst)

The respondents pointed on their analysis of the current fraud prevention measures implemented. They implement a range of measures to prevent fraud, including monitoring transactions, analysing data for anomalies and using advanced authentication technologies. The effectiveness of these measures depends on how well they are implemented and integrated into the bank's overall systems and processes. Some service providers would typically conduct regular reviews and audits of its systems and processes to identify vulnerabilities and gaps in its fraud prevention measures. They also compare their fraud prevention performance against industry benchmarks and best practices to identify areas for improvement. Internal audit activities significantly enhance fraud detection in financial institutions by providing sovereign assessment of control effectiveness and recognising operational weakness before they can be broken. Umoh, (2024).

It is also important to note that no fraud prevention measures can completely eliminate the risk of fraud. Criminals are constantly developing new tactics and techniques, so service providers must continually update their systems and processes to stay ahead of emerging threats. Additionally, fraud prevention measures must be balanced with customer convenience and ease of use to ensure that customers can access their accounts and conduct transactions without unnecessary barriers or delays.

4.3.3 Challenges Limiting Effectiveness

Four themes with supporting quotes and disconfirming cases (see 4.3.3.1 below).

Theme 1 – Management override (cited by 9 of 12)

“A director can call the reconciliation team and say ‘release that payment, I will sign later’. The policy says no, but authority wins.” (F4, Fraud Investigator)

Theme 2 – Collusion (cited by 8 of 12)

“Two people in loan processing one creates a fake customer, the other approves. Segregation of duties means nothing if they agree.” (F6, Senior Finance Officer)

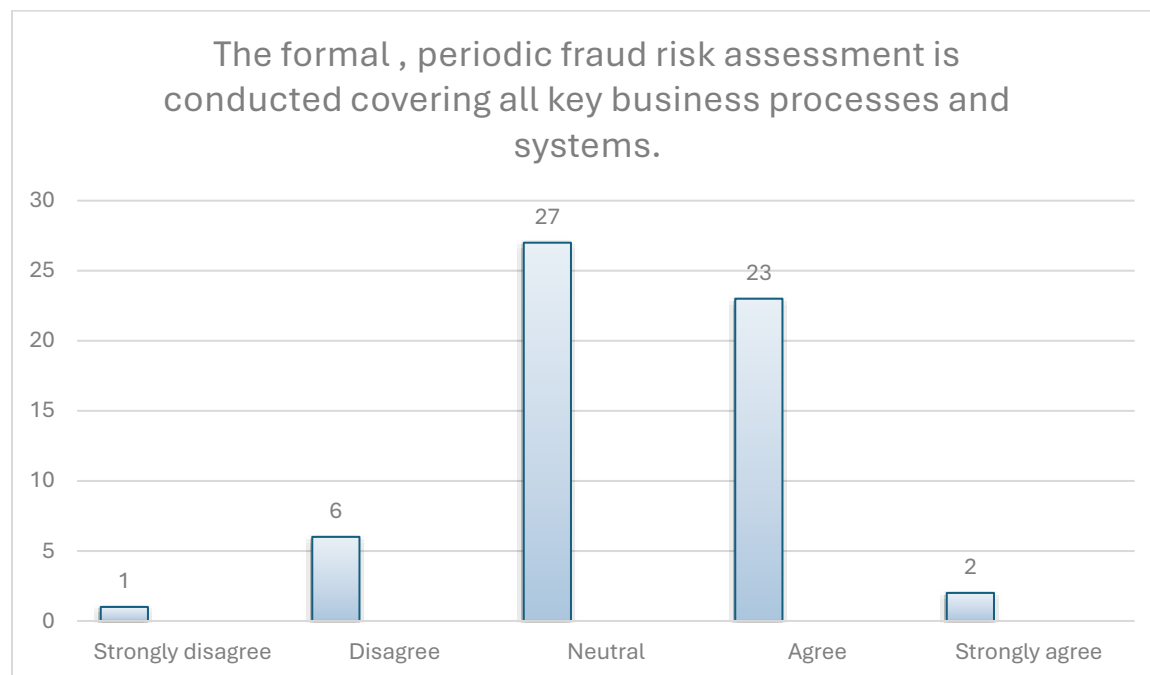
Theme 3 – Resource & competency gaps (cited by 11 of 12)

“We have three people in compliance for a bank with 200,000 customers. We still use Excel sampling no continuous monitoring.” (F12, Compliance Officer)

Theme 4 – Alert fatigue & siloed systems (cited by 10 of 12)

“Our anti-fraud software generates 500 alerts a day. 490 are false. By Friday, you ignore them all that’s when the real one comes.” (F8, Internal Audit)

Figure 4.7



Source: Research data

The findings suggest that the effectiveness of fraud risk assessments in financial institutions remains questionable despite the existence of formal assessment frameworks. Furthermore, reliance on periodic assessments creates vulnerabilities in rapidly changing environments, as static

reviews may fail to identify emerging risks between assessment cycles. This concern is reflected in the Barclays case, where evolving customer risks remained undetected for several years, resulting in significant regulatory penalties (FCA, 2025; Everest Group, 2024). The high proportion of neutral responses in the survey may therefore indicate uncertainty regarding the competence and completeness of existing risk assessment processes rather than a lack of awareness. Studies in FinTech banking and commercial banking sectors have correspondingly shown that weak risk cultures, denial of internal fraud risks and poor integration of fraud prevention measures undermine the effectiveness of risk assessments. (FinTech Banking Research, (2024); Kenyan Commercial Banks Study, (2023). Additionally, research highlights that risk assessments often become compliance-driven “tick-box” exercises disconnected from operational realities, reducing their effectiveness in detecting fraud. Indian Banking Study, (2024); Ethiopian Banking Study, (2025). The problem is further exacerbated by management override and weak control environments, over half of occupational fraud cases are linked to either absent controls or management circumvention of existing controls. (ACFE, 2024). Collectively, these findings suggest that robust fraud risk management requires dynamic, continuously monitored and culturally embedded risk assessment processes rather than periodic compliance-oriented reviews. FCA, (2025).

4.3.3.1 Disconfirming Cases (Responses that did not fit the main pattern)

Two respondents provided views that partially contradicted the dominant themes:

R2 (Senior Finance Officer, 12 years' experience) stated: “Management override is not a problem here. Our CEO has no direct system access all overrides require a four-eye committee including non-executive directors.” This is unique with the majority view. The researcher verified this with the bank's policy document (provided by F2). This proposes that one institution has effectively designed out management override, but this shows to be an outlier.

· R10 (Internal Audit, small commercial bank) disagreed with the “alert fatigue” theme: “We have a dedicated 24/7 team for alerts no fatigue. Our false positive rate is only 12% because we tuned our models to local transaction patterns.” However, the same respondent confirmed “siloed systems” as a major challenge, indicating fractional disconfirmation.

The respondents provided these four interconnected challenges which emerged repeatedly. Management override is the most cited senior executives can bypass controls or pressure subordinates to ignore red flags. Collusion between two or more employees routinely defeats segregation of duties. Resource and competency gaps mean that control functions (compliance, internal audit) are understaffed, lack forensic skills, or rely on old manual sampling instead of continuous data analysis. Finally, siloed information systems prevent a solid view of customer and employee behaviour, while the sheer volume of false positives from automated monitoring tools direct to alert fatigue and genuine fraud signals being missed.

4.3.4 Possible recommendations to failures of internal controls

Direct quotes (each recommendation is tied to at least two respondents):

“Multi-factor authentication for every transaction above \$500 not just login. That would help stop account takeover cold.” (F5 and F7 agreed)

“Real-time monitoring is expensive but necessary. We batch process daily criminals move money in minutes.” (F1, F11)

“Train staff every six months, not once a year. And test them with simulated phishing we don’t do that now.” (F4, F9)

“Share fraud intelligence with other financial institution domicile in Harare central business district. We all see different pieces of the same puzzle.” (F3, F6, F12)

The respondents gave ideas on areas that needed improvements on fraud prevention measures used by financial service sector to enhance their effectiveness in detecting and preventing fraudulent activities. Recommendations that the sector can consider:

- Implement multi-factor authentication such as two-factor authentication or biometric authentication, to verify the identity of customers. This can help prevent identity theft and account takeover.
- Monitor transactions in real-time to detect and prevent fraudulent activities such as unusual transactions or large transfers.
- The usage of machine learning algorithms to analyse customer behaviour and identify patterns that may indicate fraudulent activities.

- Conduct regular staff training to staff members on fraud detection and prevention techniques to ensure that they are equipped to identify and prevent fraudulent activities.
- Implement fraud risk evaluations to identify potential vulnerabilities and areas for improvement in their fraud prevention measures.
- Collaborate with other financial institutions to share information and best practices on fraud prevention measures.

4.4 Summary

The above data presents data from 59 questionnaires (65% response rate) and 12 interviews across Harare's financial institutions situated in the (CBD). The most common fraud types identified are asset misappropriation and financial statement fraud, followed by cyber-enabled fraud. Key internal control weaknesses include insufficient technological tools, inadequate staff fraud training, management override, employee collusion and siloed information systems. IT access controls and segregation of duties are rated most effective, while corporate ethics score lowest. Interview findings reveal that preventive measures like biometric access, duty segregation and detective controls like automated reconciliation exist, but digital channels remain vulnerable. Challenges such as alert fatigue, understaffed audit functions and outdated manual sampling limit effectiveness. Recommendations include multi-factor authentication, real-time monitoring, machine learning, regular staff training, fraud risk assessments and inter-institutional collaboration. The chapter concludes that while internal controls partially detect fraud, significant technological and oversight gaps undermine their overall effectiveness.

CHAPTER 5

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter presents a summary of the major findings derived from the data analysis in Chapter Four, draws conclusions based on the research objectives outlined in Chapter One and offers practical recommendations for improving the effectiveness of internal controls in detecting fraud within financial institutions in Harare's Central Business District. The recommendations are grounded in the empirical evidence collected and are formed within the existing body of literature on internal controls and fraud detection. The chapter concludes with suggestions for further research and a final summary.

5.1 Summary of Major Findings

The study investigated the effectiveness of internal controls in unearthing fraud within financial institutions domiciled in Harare's Central Business District. Drawing from a response rate of 65% (59 out of 92 questionnaires) and 12 semi-structured interviews, the following major findings emerged, the internal controls play a significant role in unearthing fraud within financial institutions in Harare CBD, although their effectiveness varies across fraud typologies. Financial institutions have implemented a combination of preventive and detective controls, including segregation of duties, transaction authorization limits, IT access controls, reconciliations, exception reporting and internal audits. The findings revealed that technical controls such as IT access controls and segregation of duties are highly effective in detecting fraud, particularly asset misappropriation and financial statement fraud, which were identified as the most prevalent threats. These findings are consistent with past studies which found that strong internal control systems reduce fraud opportunities and enhance fraud detection prospects in financial institutions (Wells, 2005; COSO, 2013; Amudo & Inanga, 2009). However, the study also found that management override, employee collusion, inadequate technological resources, limited forensic

competencies and alert fatigue hinder the effectiveness of internal controls. Fraud detection mechanisms are less effective when ethical culture and management oversight are compromised. ACFE, (2022) and Rae and Subramaniam (2008). Overall, the results suggest that while robust internal controls are essential for fraud detection, their success depends on a strong control environment, adequate technological support and ethical leadership. Cressey's (1953) Fraud Triangle Theory and the COSO (2013) Internal Control Framework.

5.2 Conclusions

Based on the findings presented in Chapter Four and summarized above, the following conclusions are drawn in direct response to the research objectives and sub-problems stated in Chapter One: The study concludes that internal controls play a critical role in detecting fraud within financial institutions in Harare CBD, as evidenced by the widespread usage of mechanisms such as segregation of duties, authorization controls, biometric access systems, automated reconciliations and transaction monitoring systems. These controls have proven effective in detecting traditional fraud schemes, including asset misappropriation and financial statement manipulation however, their effectiveness is limited against sophisticated fraud typologies such as cyber-enabled fraud, collusion and management override. The findings further reveal that resource constraints, skills shortages and fragmented monitoring systems significantly reduce the capacity of institutions to detect emerging fraud risks. While a positive relationship exists between robust control activities and increased fraud detection frequency. Also, weaknesses in digital banking controls continue to create opportunities for fraudsters. Overall, the study demonstrates that internal controls remain a necessary but insufficient mechanism for fraud detection unless they are continuously updated, adequately resourced and integrated with advanced fraud monitoring techniques. These findings are consistent with previous studies which found that strong internal control systems significantly improve fraud detection and prevention in financial institutions, although their effectiveness depends on proper implementation and adaptation to emerging risks. Njanike et al., (2011); Tembo, (2015); Oronde, (2022); Skousen et al., (2009).

5.3 Recommendations

Based on the findings and conclusions, the following recommendations are suggested to enhance the effectiveness of internal controls in unearthing fraud within financial institutions in Harare's

Central Business District. These recommendations are examined in the light of suggested applications and are supported by relevant past research.

5.3.1 Recommendations for Financial Institutions

5.3.1.1 Invest in Advanced Technological Tools and Data Analytics Capabilities

The Insufficient of technological tools or data analytics was identified by 42 respondents as the most prevalent corporate setups issues. Alert fatigue and siloed systems were cited by 10 of 12 interviewees as major challenge. Financial institutions should transition from manual sampling and batch processing to real-time, AI-driven transaction monitoring systems. Specifically Implement machine learning algorithms that adapt to local transaction patterns to reduce false positive rates (as demonstrated by the outlier institution in this study achieving a 12% false positive rate through locally-tuned models).Deploy continuous monitoring systems rather than daily batch processing, recognizing that "criminals move money in minutes" (F1, F11).Integrate siloed information systems to create a solid view of customer and employee behaviour across all channels. Deloitte (2020),'African banks often lag in adopting AI-driven transaction monitoring', creating a skills and tools gap. the harnessing machine learning and artificial intelligence for early fraud detection among banks in Harare, Zimbabwe, from internal auditors' perspective. Chingwaro, Muchowe, and Njaya, (2024)

5.3.1.2 Strengthen Controls in Digital Channels

The respondents constantly noted that controls are robust in traditional banking operations and "thinner in newer digital channels," where onboarding and transaction monitoring rely heavily on third-party systems. Implement (MFA) multi-factor authentication for every transaction above a threshold (e.g., USD \$500), not just for login. As F5 and F7 agreed, "That would stop account takeover. "Reduce reliance on third-party KYC systems by developing or acquiring internal verification capabilities. Conduct regular security assessments of digital onboarding processes and mobile banking platforms. There is the need for enhanced digital channel controls. Manhide and Nkomo, (2023). The guidance on AML & CFT compliance for fintech's and financial institutions in Zimbabwe. Vove ID, (2025).

5.3.1.3 Address Management Override Through Structural Controls

Management override was cited by 9 of 12 interviewees as a significant challenge, with one institution demonstrating that effective design can eliminate this risk. Adopt the outlier institution's

model where "all overrides require a four-eye committee including non-executive directors" and the CEO has no direct system access. Specific actions contain to remove direct system access for senior executives to transaction-processing systems. Implement automated logging of all override attempts with mandatory weekly review by the audit committee. This recommendation aligns with Cunningham's, (2004) analysis on the appeal and limits of internal controls to fight fraud, and with the COSO, (2013) emphasis on the control environment as the foundation of all other components.

5.3.1.4 Enhance Fraud Awareness Training Programs

Inadequate staff training on fraud awareness was identified by 35 respondents as a major weakness. Conduct fraud awareness training every six months rather than annually, as recommended by F4 and F9. Include simulated phishing exercises to test and reinforce learning. Integrate fraud-related training based on employee job responsibilities to enhance efficiency. Gates, Prachyl and Sullivan, (2016) and Peltier-Rivest and Lanoue, (2015). Ensure training covers evolving fraud typologies, particularly social engineering and cyber-enabled fraud. Employees who are well-informed about anti-fraud policies and measures are better equipped to identify potential fraud risks promptly. Henry, (2016). A comprehensive guidance on fraud auditing and forensic accounting training approaches is of paramount importance. Singleton and Singleton, (2010)

5.3.1.5 Increase Resources for Control Functions

Understaffed or under-resourced internal audit or compliance departments were cited by 20 respondents, with qualitative data revealing extreme ratios (e.g., "three people in compliance for a bank with 200,000 customers"). Conduct workload assessments for compliance, internal audit and fraud investigation units to establish evidence-based staffing levels. Invest in continuous professional development for control function staff, particularly in forensic data analytics and cyber-fraud investigation. Consider centralized or shared-service models for smaller institutions to achieve economies of scale in fraud detection capabilities. Halaku (2024) studied the effect of internal control mechanisms on fraud prevention in deposit-taking savings and credit cooperative societies in Kenya, demonstrating that resource adequacy is a critical success factor. Devi (2026) empirically investigated management accounting control systems and fraud risk mitigation, supporting the resource-based view of control effectiveness.

5.3.1.6 Mandate Technology Upgrades and Establish Minimum Standards

The FIU (2024) in its reports acknowledged that enforcement actions fall short of demonstrating an effective national AML/CFT system. Issue obligatory directives requiring financial institutions to implement real-time transaction monitoring systems with detailed false-positive rate targets. Create minimum staffing ratios for compliance and internal audit functions based on customer volume and transaction value. Mandate annual independent assessments of internal control effectiveness for fraud detection, with results reported to the FIU. The Sarbanes-Oxley Act of 2002 (SOX) provided the legislative precedent for mandating internal control requirements to reduce corporate misconduct and fraud. Gao and Jia, (2015). The value of forensic auditing of related party transactions is used as a strategy for averting fraud in Zimbabwean listed financial institutions. Kapesa, (2026)

5.3.1.7 Facilitate Inter-Institutional Intelligence Sharing

Interview respondents recommended sharing fraud intelligence with other financial institutions because "we all see different pieces of the same puzzle" (F3, F6, F12). Establish a secure, regulated platform for financial institutions to share anonymized fraud intelligence, including emerging modus operandi and suspect identifiers. Mandate participation in this platform as a condition of licensing. Ensure the platform includes protections against regulatory retaliation for good-faith sharing. The ACFE, (2022) Report to the Nations highlighted that organizations with formal fraud intelligence sharing mechanisms detect fraud 33% faster than those without such mechanisms.

5.3.2 Recommendations for Future Research

Based on the limitations and findings of this study, the following areas are suggested for future investigation:

- **Longitudinal Study of Internal Control Effectiveness:** A study tracking the same institutions over 3-5 years to assess whether regulatory interventions and technology investments lead to measurable improvements in fraud detection rates.
- **Comparative Study Across Zimbabwean Cities:** This study was limited to Harare CBD. Future research should compare fraud patterns and control effectiveness in Bulawayo, Mutare, Gweru, and other urban centres to assess generalizability.

- Quantitative Study of the Fraud Diamond in Zimbabwe: This study found qualitative support for the Fraud Diamond Theory's "capability" element. A quantitative study measuring the relative predictive power of pressure, opportunity, rationalization, and capability in the Zimbabwean context would contribute to theory development.
- Cost-Benefit Analysis of AI-Driven Fraud Detection: As institutions consider investing in machine learning and real-time monitoring systems, a rigorous cost-benefit analysis specific to the Zimbabwean financial sector would inform resource allocation decisions.
- Study of Whistleblowing Mechanisms Effectiveness: Given that collusion was identified as a major challenge, research on the effectiveness of anonymous reporting channels and whistleblower protection in Zimbabwean financial institutions is warranted.

5.4 Summary

This study investigated the effectiveness of internal controls in detecting fraud within financial institutions in Harare's central business district, Zimbabwe. Motivated by persistent fraud despite existing regulatory frameworks such as the Money Laundering and Proceeds of Crime Act and RBZ guidelines. The research was grounded in the Fraud Triangle Theory (Cressey, 1953), which identifies pressure, opportunity and rationalization as enablers of fraud and the Fraud Diamond Theory (Wolfe & Hermanson, 2004), which adds capability as a fourth element. Previous studies have documented weak internal controls in Zimbabwean banks, (Tembo, 2015) and noted that fraud losses globally equate to approximately 6.05% of GDP (Gee & Button, 2019). Using a mixed-methods design with 59 questionnaires and 12 semi-structured interviews, the study found that asset misappropriation and financial statement fraud were the most prevalent types, while key challenges limiting control effectiveness included insufficient technological tools (cited by 42 respondents), inadequate staff training (35), management override (29), and collusion (34) findings consistent with the past studies of Mugari et al, (2016) on cybercrime in Harare banks and Oronde, (2022) on weak internal controls in Kenya. Although IT access controls and segregation of duties were rated as relatively effective, corporate ethics scored lowest. The study concluded that while internal controls partially detect fraud, significant gaps in technology, resources and oversight breed fraud in financial institutions. Drawing the following recommendations, multi-factor authentication, real-time transaction monitoring, regular fraud training and inter-institutional intelligence sharing.

References

- ACFE (2022). Report to the Nations: Occupational Fraud 2022. Association of Certified Fraud Examiners.
- ACFE (2024). Occupational Fraud 2024: A Report to the Nations. Association of Certified Fraud Examiners.
- Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2019). *Fraud examination* (6th ed.). Cengage.
- Allison, R. M. (2001). Markov chain sampling methods for Dirichlet process mixture models. *Journal of Computational and Graphical Statistics*, 10(2), 249–265.
- Amudo, A., & Inanga, E. L. (2009). Evaluation of internal control systems: A case study from Uganda. *International Research Journal of Finance and Economics*, 27, 124–144.
- Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, 11(4), 589–597.
- Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications.
- Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.
- Campbell, D. R., Campbell, M., & Adams, G. W. (2006). Adding significant value with internal controls. *The CPA Journal*, 76(6), 20.
- Chingwaro, L., Muchowe, R. M., & Njaya, T. M. (2024). Harnessing machine learning and artificial intelligence for early fraud detection among banks in Harare, Zimbabwe: Internal auditors' perspective. *Management Review – MMR*.
- COSO (1992). *Internal control – integrated framework*. Committee of Sponsoring Organizations of the Treadway Commission.
- COSO (2013). *Internal control – integrated framework*. Committee of Sponsoring Organizations of the Treadway Commission.
- Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

- Creswell, J. W. (2007). *Qualitative inquiry and research design* (3rd ed.). SAGE Publications.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approach* (5th ed.). SAGE Publications.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- Cunningham, L. A. (2004). The appeal and limits of internal controls to fight fraud, terrorism, other ills. *Boston College Law Review*, 46(1), 1–66.
- Devi, K. (2026). Management accounting control systems and fraud risk mitigation: An empirical investigation. *Journal of African Development*, 7(1), 127–138.
- Everest Group (2025). Research on financial transaction complexity and reactive control limitations. In T. McCrossan, “Hiding in plain sight: The biggest risks CFOs don’t see coming,” Forbes Finance Council.
- Fabiyi, O. O. (2025). Internal control system and fraud prevention in Nigerian deposit money banks. core.ac.uk.
- Financial Conduct Authority (FCA) (2025). Findings of thematic review into firm risk assessment processes and controls (published 17 November 2025).
- Financial Intelligence Unit (FIU) (2024). 2024 annual report. Harare: FIU.
- Financial Intelligence Unit (FIU) (n.d.). Overview. Available at: www.fiu.co.zw/index.php/overview/ (Accessed: 6 April 2026).
- Gee, J., & Button, M. (2019). *The financial cost of fraud 2019: The latest data from around the world*. Crowe Global.
- Halaku, J. J. N. (2024). Effect of internal control mechanism on fraud prevention of deposit-taking savings and credit cooperative societies in Kenya (Thesis). University of Nairobi.
- Jaggi, B., & Leung, S. (2007). Impact of family dominance on monitoring of earnings management by audit committees: Evidence from Hong Kong. *Journal of International Accounting, Auditing and Taxation*, 16(1), 27–50.

- Johnson (2012). [Source not located – consult supervisor for alternative or verification.]
- Kanu, N. O., Ugwuodioha, O., Onmonya, L. O., & Azu, N. P. (2025). Effectiveness of internal control system on fraud detection in Nigerian public sector: A study of the Central Bank of Nigeria. *Veredas do Direito*, 23(4), 1–25.
- Kapesa, T. (2025). Forensic auditing of related party transactions: A strategy for averting fraud in Zimbabwean listed banks. *Copernican Journal of Finance & Accounting*.
- Kapesa, T. (2026). Forensic auditing of related party transactions: A strategy for averting fraud in Zimbabwean listed banks. *Copernican Journal of Finance & Accounting* (forthcoming).
- Manhide, T. C., & Nkomo, D. J. (2023). Determination of factors influencing the upsurge of electronic banking frauds in Zimbabwe. *Journal of Research and Innovation for Sustainable Society*, 5(2).
- Mugari, I., Gona, T., Maunga, M., & Chiyambiro, R. (2016). Cybercrime in Zimbabwe's financial sector: Prevalence and countermeasures. *International Journal of Cyber Criminology*, 10(1), 45–59.
- Mutanda, B., & Chrispen, M. (2023). Towards a cyber resilient banking system: Effectiveness of cyber fraud risk management strategies adopted by commercial banks in Zimbabwe. *Studies and Scientific Researches. Economics Edition*, (37).
- Mwai, D. K., Kuria, A., & Musili, L. W. (2025). Preventive fraud risk management and fraud incidence: Evidence from commercial banks in Kenya (2020–2024). *International Journal of Research and Innovation in Social Science*, 9(11), 1470–1480.
- Nehanda Radio (2025). Trio busted in RBZ exhibition fund email scam, facing money laundering charges. *Nehanda Radio*, 18 September. Available at: nehandaradio.com (Accessed: 6 April 2026).
- Njanike, K., Dube, T., & Mashayanye, E. (2011). The effectiveness of forensic auditing in detecting, investigating, and preventing bank frauds. *Journal of Sustainable Development in Africa*, 13(7), 405–425.

- Njanike, K., Mutengezanwa, M., & Gombarume, F. B. (2011). Internal controls in ensuring good corporate governance in financial institutions. *Annals of the University of Petrosani: Economics*, 11(3), 187–196.
- Norman-Maillet, C. (2026). “We don’t have any internal fraud...”: Internal fraud and its risks to FinTech banks (Doctoral thesis). University of Portsmouth.
- Oronde, M. O. (2022). Effect of internal control systems on fraud prevention in commercial banks in Kenya. *International Journal of Finance and Accounting*, 7(2), 45–58.
- Oronde, P. (2022). Factors hindering fraud prevention strategies in Kenyan financial institutions. *Journal of Financial Crime*, 29(3), 712–728.
- Pinho, C. (2015). Implementation of internal control systems to combat money laundering and financing of terrorism: An applied exploratory study to the Angolan financial sector. *International Journal of Business and Social Research*, 5(7), 23–35.
- Rae, K., & Subramaniam, N. (2008). Quality of internal control procedures and employee fraud. *Managerial Auditing Journal*, 23(2), 104–124.
- Raut, S. (2025). Occupational fraud in family and non-family businesses: A mixed-methods study using expert perceptions (Doctoral thesis). Bond University.
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson.
- Singleton, T. W., & Singleton, A. J. (2010). *Fraud auditing and forensic accounting* (4th ed.). John Wiley & Sons.
- Skousen, C. J., Smith, K. R., & Wright, C. J. (2009). Detecting and predicting financial statement fraud: The effectiveness of the fraud triangle and SAS No. 99. In *Corporate governance and firm performance* (pp. 53–81). Emerald Group Publishing.
- Soni, L., & Mangala, D. (2025). Preventing and detecting internal fraud risk: A critical analysis of the anti-fraud tools used by the Indian banking industry. *Journal of Money Laundering Control*, 28(2), 424–441.

Tembo, J. (2015). An investigation into the causes of fraud in banks in Zimbabwe. *Journal of Financial Crime*, 22(4), 454–467.

Tembo, N. (2015). An evaluation of internal controls in Zimbabwean banking institutions and their role in fraud prevention (Unpublished master's dissertation). University of Zimbabwe.

Tesfaye, F. A. (2024). An exploration of internal control system of Ethiopian banks (Doctoral dissertation). Liberty University.

Umoh, B. E. (2024). Internal audit functions and fraud prevention and detection in financial institutions: An analytical study of Access Bank Plc (2017–2022). *SSRN Electronic Journal*.

Vove ID (2025). AML & CFT compliance in Zimbabwe: 2026 guide for fintechs and financial institutions. Available at: <https://blog.voveid.com/aml-cft-compliance-in-zimbabwe-2025-guide-for-fintechs-and-financial-institutions/> (Accessed: 9 April 2026).

Wells, J. T. (2005). *Principles of fraud examination*. John Wiley & Sons / Association of Certified Fraud Examiners.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.

Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). SAGE Publications.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.

Bindura University of Science Education

P. Bag 1020

Bindura

Zimbabwe

To whom it may concern.

RE: REQUEST FOR RESEARCH ASSISTANCE.

I am JOSEPH JAMES CHINHAMU, an undergraduate student at Bindura University of Science Education. I am studying for a Bachelor of Commerce (Honours) Degree in Financial Intelligence. As part of my studies, I am conducting a research study titled **the effectiveness of internal controls in unearthing fraud in financial institutions in Zimbabwe. A survey of Harare (CBD).**

I would be tremendously grateful for your willingness to take part in this endeavor by providing an overview of the dangers posed by Fraudulent activities in the financial service sector. Please help me out by filling out the accompanying questionnaire.

It is completely up to you whether or not you participate in this survey, and you are authorized to do so without experiencing any penalties, at any moment. Also, you are informed that participating in the study will not provide you with any financial or other benefits. I assure that the data gathered will only be utilized for this project as well as being handled with the highest level of confidentiality.

Yours Faithfully

Joseph Chinhamu

APPENDIX 2: QUESTIONNAIRE FOR FINANCIAL SERVICE PROVIDER RESPONDENTS

SECTION A: GENERAL INFORMATION AND FRAUD LANDSCAPE

(Please tick ✓ the appropriate box or fill in the blank)

1. Type of financial institution you work for:

- ☐ Commercial Bank ☐ Microfinance Institution ☐ Building Society ☐ Insurance Company ☐ Securities/Asset Management Firm ☐ Mobile Money/Payment Service Provider
☐ Other (please specify) _____

2. Your primary functional area:

- ☐ Internal Audit ☐ Risk Management ☐ Compliance ☐ Fraud Investigation ☐ Senior Finance (CFO, Financial Controller, Finance Manager) ☐ Other (specify) _____

3. How many years of experience do you have in the financial services sector?

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

4. In your opinion, how prevalent is occupational fraud in the Harare CBD financial services sector?

- ☐ Very high ☐ High ☐ Moderate ☐ Low ☐ Very low

5. Which category of fraud poses the greatest threat to your institution? (Select the top two)

- ☐ Asset misappropriation (cash, inventory) ☐ Financial statement fraud ☐ Corruption/bribery ☐ Cyber-enabled fraud ☐ Customer/third-party fraud ☐ Other

SECTION B: CONTROL ENVIRONMENT AND ETHICAL CULTURE

(Indicate your level of agreement with each statement: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree)

No. Statement 1 2 3 4 5

B1 The board and senior management demonstrate a strong commitment to integrity and ethical values. ☐ ☐ ☐ ☐ ☐

B2 A formal, well-communicated anti-fraud policy exists and is enforced consistently across the organisation. ☐ ☐ ☐ ☐ ☐

B3 Management consistently communicates that internal control responsibilities must be taken seriously. ☐ ☐ ☐ ☐ ☐

B4 Hiring and promotion practices include adequate background screening to mitigate the risk of employing fraudulent individuals. ☐ ☐ ☐ ☐ ☐

B5 Employees are encouraged and feel safe to report suspected fraudulent activities without fear of retaliation. ☐ ☐ ☐ ☐ ☐

B6 There is a clear segregation of duties between those who authorise transactions, record them, and maintain custody of assets. ☐ ☐ ☐ ☐ ☐

SECTION C: RISK ASSESSMENT AND CONTROL ACTIVITIES

(1 = Strongly Disagree → 5 = Strongly Agree)

No. Statement 1 2 3 4 5

C1 A formal, periodic fraud risk assessment is conducted covering all key business processes and systems. ☐ ☐ ☐ ☐ ☐

C2 The fraud risk assessment explicitly considers the potential for management override of controls. ☐ ☐ ☐ ☐ ☐

C3 Preventive controls (e.g. multi-level approvals, physical safeguards, IT access restrictions) are effective in blocking fraudulent attempts before they occur. ☐ ☐ ☐ ☐ ☐

C4 Detective controls (e.g. reconciliations, exception reports, surprise audits) reliably flag anomalies that could indicate fraud. ☐ ☐ ☐ ☐ ☐

C5 Reconciliations (bank, ledger, system-to-system) are performed in a timely manner and independently reviewed. ☐ ☐ ☐ ☐ ☐

C6 IT application controls (input validation, automated alerts, access logs) are properly configured to detect unusual transaction patterns. ☐ ☐ ☐ ☐ ☐

C7 Dual authorization or maker-checker processes are mandatory for high-value or sensitive transactions. ☐ ☐ ☐ ☐ ☐

C8 Physical controls over cash, blank cheques, and sensitive documents are adequate to prevent unauthorized access. ☐ ☐ ☐ ☐

SECTION D: INFORMATION, COMMUNICATION AND WHISTLE-BLOWING MECHANISMS

(1 = Strongly Disagree → 5 = Strongly Agree)

No. Statement 1 2 3 4 5

D1 The institution has established secure and anonymous whistle-blowing channels (hotline, email, web portal). ☐ ☐ ☐ ☐ ☐

D2 Employees are regularly trained on identifying red flags of fraud and how to report them.
☐ ☐ ☐ ☐ ☐

D3 Information on control failures and fraud incidents is shared promptly with relevant stakeholders (audit committee, risk, compliance). ☐ ☐ ☐ ☐ ☐

D4 Management actively communicates the results of fraud investigations to enhance awareness and deterrence. ☐ ☐ ☐ ☐ ☐

D5 Data analytics and continuous auditing tools are employed to proactively identify suspicious transactions. ☐ ☐ ☐ ☐ ☐

D6 There is effective coordination between internal audit, risk management, compliance, and fraud investigation units. ☐ ☐ ☐ ☐ ☐

SECTION E: MONITORING, OVERALL EFFECTIVENESS AND CHALLENGES

(1 = Strongly Disagree → 5 = Strongly Agree, unless otherwise indicated)

No. Statement 1 2 3 4 5

E1 The internal audit function has sufficient independence, resources, and competence to assess fraud-related controls. ☐ ☐ ☐ ☐ ☐

E2 Internal audit reports routinely include recommendations that strengthen the organisation's ability to detect fraud. ☐ ☐ ☐ ☐ ☐

E3 Corrective actions on identified control weaknesses are implemented in a timely manner.
☐ ☐ ☐ ☐ ☐

E4 Overall, the existing internal control system is effective in unearthing fraud in a timely manner. ☐ ☐ ☐ ☐ ☐

E5. What are the biggest obstacles to effective fraud detection through internal controls in your institution? (Select all that apply)

- ☐ Management override of controls
- ☐ Inadequate staff training on fraud awareness
- ☐ Insufficient technological tools/data analytics
- ☐ Collusion among employees or with third parties
- ☐ Low prioritisation of fraud risk by senior management
- ☐ Understaffed or under-resourced internal audit/compliance departments
- ☐ Poorly designed or outdated control procedures
- ☐ Lack of independence of control functions
- ☐ Other (please specify) _____

E6. In your view, which two internal control components have contributed the most to uncovering actual fraud cases in your institution?

- ☐ Ethical culture at the top
- ☐ Whistle-blower tips/reporting mechanisms
- ☐ Proactive data analytics/monitoring
- ☐ Routine reconciliations and exception reports
- ☐ Surprise audits/inspections
- ☐ IT access controls and system logs
- ☐ Segregation of duties
- ☐ Other _____

E7. What improvements would you recommend to strengthen internal controls for better fraud detection in the Harare financial services environment?

.....

APPENDIX 3: INTERVIEW GUIDE

Theme 1: Identification of Internal Controls in Place

(Objective: Identify the internal controls currently operating in the organization.)

1. Can you describe the key internal control mechanisms your institution uses to safeguard assets and ensure the integrity of financial reporting?
2. Which preventive controls (e.g., segregation of duties, authorization limits, access restrictions) and detective controls (e.g., reconciliations, exception reports, surprise audits) are formally documented in your policies?
3. How are these controls passed to staff, and how is compliance to the system of controls monitored on a daily basis?

Theme 2: Extent to Which Internal Controls Detect Fraud

(Objective: Assess how effectively existing controls unearth fraudulent activity.)

4. In your experience, how successful have your internal controls been in identifying actual or attempted fraud? Also, can you share an example without breaching confidentiality?
5. What types of fraud are most and least likely to be caught by the controls you currently have?
6. When a control measure flags a potential irregularity, how quickly and thoroughly is it typically investigated?

Theme 3: Challenges That Limit the Effectiveness of Internal Controls

(Objective: Understand the obstacles that prevent controls from detecting fraud.)

7. What are the main reasons internal controls fail to detect fraud in your organization procedural, human, or technological?
8. To what extent do factors like management override, collusion, resource constraints, or employee familiarity with control gaps weaken detection?

9. How does the rapidly evolving digital landscape (e.g., real-time payments, fintech partnerships) challenge your legacy control environment?

Theme 4: Recommendations for Adopting More Effective Controls

(Objective: Propose actionable improvements to the control framework.)

10. If you could change three things about your current internal control system to better unearth fraud, what would they be?

11. What role should technology play in strengthening fraud detection, and what barriers stand in the way of implementation?

12. Beyond tools, what cultural or governance shifts would you recommend to make controls truly effective?

APPENDIX 4: TURNITIN REPORT

Joseph Chinhamu Joseph

b210783b_joseph_chinhamu_research_

 DISSERTATION PLAGIARISM CHECK

Document Details

Submission ID

trncid::2945394515028

Submission Date

Jun 21, 2026, 1:42 PM GMT+2

Download Date

Jun 22, 2026, 9:13 AM GMT+2

File Name

b210783b_joseph_chinhamu_research_.pdf

File Size

560.5 KB

54 Pages

15,049 Words

87,974 Characters



Page 1 of 63 - Cover Page

Submission ID - trncid::2945394515028



Page 2 of 63 - Integrity Overview

Submission ID - trncid::2945394515028

13% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

-  **136 Not Cited or Quoted 11%**
Matches with neither in-text citation nor quotation marks
-  **28 Missing Quotations 3%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 9%  Internet sources
- 3%  Publications
- 12%  Submitted works (Student Papers)