BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY

AN ASSESSMENT OF FRAUD CONTROL MEASURES IN THE ZIMBABWEAN BANKING SECTOR. A CASE OF ZB BANK (BINDURA BRANCH) FOR THE PERIOD OF 2020-2023.

NATALIA LUCIA MUSIYIWA

B202076B

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

APRIL 2024

RELEASE FORM

NAME OF AUTHOR: NATALIA LUCIA MUSIYIWA

STUDENT NUMBER: B202076B

TITLE OF PROJECT: AN ASSESSMENT OF FRAUD CONTROL MEASURES IN THE ZIMBABWEAN BANKING SECTOR. A CASE OF ZB BANK (BINDURA BRANCH) FOR THE PERIOD OF 2020-2023.

DEGREE TITLE: BACHELOR OF COMMERCE HONOURS DEGREE IN FINANCIAL INTELLIGENCE

YEAR GRANTED: 2024

Permission is hereby granted to Bindura University library to produce single copies of this project for research purposes only. However, no one else is allowed to reproduce or distribute the project, or share large parts of it, without the author's explicit permission. The library can lend or sell these copies for scholarly or scientific research, but that is the only exception.

SIGNED ---

PERMANENT ADDRESS: HOUSE NUMBER 9029
102 CRESCENTS
GLENVIEW 8
HARARE

APPROVAL FORM

Title of Dissertation: AN ASSESSMENT OF FRAUD CONTROL MEASURES IN THE ZIMBABWEAN BANKING SECTOR. A CASE OF ZB BANK (BINDURA BRANCH) FOR THE PERIOD OF 2020-2023.

To be completed by the 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)

To be completed by the Supervisor: This dissertation is suitable for submission to the faculty. This dissertation should be checked for conformity with the faculty guidelines

____

____

(Signature of Supervisor)

(Date)

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

____

____

(Signature of the Chair)

(Date)

DEDICATION

To my parents, Mr and Mrs Musiyiwa, I recognise your sacrifices to support me in my educational pursuits. Thank you for your prayers, unwavering love, encouragement and guidance. Words are not enough to express my gratitude.

ABSTRACT

Fraud has become a prevalent and enduring problem in the banking sector of Zimbabwe, posing substantial risks to the stability, credibility, and reliability of financial institutions. Reports of fraudulent activities persist, prompting concerns about the sufficiency and efficacy of current control mechanisms. Therefore, this research is going to assess the fraud control measures in place within Zimbabwe's banking sector, identifying any weaknesses and propose enhancement to strengthen the resilience of the financial system. The researcher used a single case study design to collect primary data using research questionnaires. The ZB Bank was used to represent commercial banks in Zimbabwe and has been used as a case study. The results obtained will be applicable to other banks. A sample of ten respondents on the questionnaire was obtained. The data was analysed, and interpreted using Microsoft excel and SPSS and was presented using charts, graphs and tables. The research findings revealed that opportunities, rather than financial need, serves as the primary motivation for fraud within the banking system. Also, the study identified various control measures implemented by ZB Bank to manage fraudulent activities. Finally, it was recommended that financial institutions enhance technological solutions by leveraging advanced technological measures such as real-time fraud monitoring systems, biometric authentication and two-factor authentication. Also, strengthen internal controls by continuously reviewing and enhancing internal control mechanisms to address the identified opportunities for fraud. Also, banks should focus on organisational learning, customer education and awareness and collaborate with consultants.

ACKNOWLEDGEMENTS

The epic task of preparing and producing this research project could not have been a success had it not been the dedication, commitment, expertise, effort, support and care exercised by the lecturers at the Bindura University of Science Education, especially those in the faculty of commerce, prior, during and after the research exercise.

My Project supervisor -for the guidance throughout the project. She devoted much of her precious time towards the success of this project. She would always give words of encouragement whenever I seemed to be tiring.

Long live! My parents, Mr and Mrs Musiyiwa- for forgoing their needs to pave the way for my studies and for their unwavering support and encouragement. I love you.

Last but not least, I thank my colleagues and classmates for the input they made to this project. It really counted. Stay blessed.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ACRONYMS

CHAPTER I

INTRODUCTION

1.0 Introduction

This study will provide a comprehensive assessment of fraud control measures in the Zimbabwean banking sector, shedding light on the strengths and weaknesses of existing frameworks. This chapter is divided into several sections, starting with an introduction, background of the study, statement of the problem, aim of the study, research objectives, research questions, assumptions, delimitations, limitations of the study, definition of terms and summary. This study aims to contribute to developing strategies and policies that can enhance the banking sector's resilience and mitigate the risks associated with fraud. Ultimately, the findings of this research will serve as a valuable resource for stakeholders seeking to safeguard the integrity and stability of the Zimbabwean financial system

1.1 Background of the study

In Zimbabwe, the banking sector plays a vital role in the country's economy, connecting savers and borrowers, supporting economic development, and providing essential financial services to a wide range of entities, including individuals, businesses, and the government. However, the sector has encountered numerous obstacles in recent years, including economic volatility, currency instability, and regulatory changes. The "Africa Fraud Barometer 2011" and the "Ernst & Young Africa Attractiveness survey 2012" forecast that Zimbabwe may face challenges in attracting foreign investment. The country faces fraud and financial difficulties, including embezzlement, employee dishonesty, and a lack of internal controls. These issues are often exacerbated by economic downturns, which can lead to organisational restructuring, weakening internal controls and placing financial pressure on employees.

Fraud and corruption are significant factors that deter investors from doing business in Africa. The KPMG report shows that in Zimbabwe, fraud cases in 2011 totalled $1.2 billion, which accounted for 32 percent of total fraud cases in Africa at $3.7 billion. Zimbabwe had the second-highest number of fraud cases in the region, behind Nigeria. These cases significantly impact the economy, as they reduce investor confidence and make it difficult for businesses to operate. According to Muradzikwa (2009), people in Zimbabwe have defrauded their employers by colluding with third-party service providers to inflate the cost of repairs on damaged vehicles. In a separate case, Chidavaenzi (2013) reported that a messenger was jailed for fraud, after adopting a method to defraud his employer. The court stated that the accused had become a repeat offender and should not be surprised by the consequences of his actions.
The RBZ Report (2016) identified the 2003-2004 financial turmoil in Zimbabwe as being caused by several factors relating to fraud, including inadequate risk management systems, inappropriate business practices, and poor accounting standards. These factors led to inaccurate financial statements, insider loans that were not being repaid, and chronic liquidity problems. The report noted that rapid expansion and creative accounting exacerbated these issues, which increased the audit risk. This study aims to examine the main factors contributing to workplace fraud in Zimbabwe, with a focus study aiming to investigate the main factors contributing to workplace fraud in Zimbabwe, focusing on the "Fraud triangle" theory. The study also aims to provide recommendations on detecting potential fraud and designing better risk management strategies. This research could be of interest to academics, practitioners, and other stakeholders in the corporate world, as it brings a new perspective to the study of fraud risk management and auditing.

1.2 Statement of the problem

Mackevičius and Giriūnas (2013) stated that individuals who commit fraud are always searching for more efficient and sophisticated methods. They investigate a company's internal and external environments, including accounting and internal control systems, financial conditions, and operational results. They also evaluate a number of other factors in order to find ways to commit fraud more effectively.
Fraud has emerged as a prominent and persistent issue within the Zimbabwean banking sector, posing significant threats to financial institutions' stability, integrity, and trustworthiness. Despite the implementation of various fraud control measures, the effectiveness of these measures remains uncertain. Instances of fraudulent activities continue to be reported, raising concerns about the adequacy and efficiency of existing control mechanisms. Consequently,

there is a pressing need to assess the fraud control measures within the Zimbabwean banking sector, identify weaknesses, and propose improvements to enhance the financial system's resilience. By examining the effectiveness of current measures and identifying areas for improvement, this study aims to contribute to the development of more robust and proactive strategies for combating fraud, safeguarding the financial system, and restoring public trust in the banking sector.

1.3 Aim of the study

To assess the effectiveness of fraud control measures implemented by banks in the Zimbabwean banking sector, mainly focusing on ZB bank.

1.4 Research objectives

To identify the underlying causes of fraud incidents in banking systems, specifically ZB bank
To identify the existing fraud control measures implemented by ZB bank.
To identify any weaknesses or gaps in the fraud control measures employed by ZB bank.
To provide recommendations for enhancing fraud control measures in Zimbabwean banks.

1.5 Research questions

What are the causes of fraud incidents in ZB bank?
What fraud control measures were implemented by the ZB bank?
What were the weaknesses identified in the fraud control measures employed by ZB bank?
What recommendations can be made to enhance the fraud control measures in Zimbabwean banks?

1.6 Significance of the study

To the researcher

This study is an important milestone for the researcher to earn a bachelor of commerce honours degree in financial intelligence. It's part of the overall process of gaining knowledge and skills in the field of financial intelligence, intending to prevent and reduce fraud. By conducting this study, the researcher will have the opportunity to engage with banking professionals, regulatory authorities, and other stakeholders. This can help the researcher develop their professional network and create potential collaboration opportunities, which could lead to career advancement. The researcher hopes that these connections will help them gain a deeper understanding of the financial industry and become a more knowledgeable professional.

To the university

This study contributes to the university's knowledge base by generating new insights and empirical evidence on fraud control measures in the banking sector. Conducting this type of research shows the university's dedication to conducting relevant and impactful research. The study will demonstrate the university's expertise in banking, finance, and fraud prevention, which could boost its academic reputation and position it as a leader in the field. The findings of the study may also benefit the university by raising awareness of its research capabilities and encouraging more students to enrol in related programs.

To the financial institutions

The results of this study can help financial institutions in Zimbabwe identify gaps and weaknesses in their fraud control mechanisms. By evaluating the effectiveness of these mechanisms, the study can provide insight into how they can be improved to reduce the risks associated with fraud. This can ultimately help institutions better protect themselves and their customers from financial losses due to fraud.

1.7 Assumptions

- The reported cases of fraud in the Zimbabwean banking sector were indicative of the actual occurrence and prevalence of fraudulent activities.
- Zimbabwe's regulatory framework and legal environment were conducive to effective fraud control measures.
- The selected banking institution was representative of the broader Zimbabwean banking sector.
- The information provided by banking institutions concerning their fraud control measures was accurate and comprehensive.
- The banking professionals who participated in interviews or surveys provided honest and accurate responses.

1.8 Delimitations

The study focused specifically on the Zimbabwean banking sector and may not have encompassed fraud control measures and practices in other countries or regions. Consequently, the findings and conclusions were interpreted within the context of the Zimbabwean banking system, and may not have been directly applicable to other jurisdictions. The study could have included a limited number of banking institutions due to practical constraints such as time, resources, and access to data. The findings and conclusions drawn from the selected sample should have been generalised cautiously, considering the potential variations and diversity within the broader banking sector.

1.9 Limitations

The study's findings and analysis could have been limited by the availability and accessibility of relevant data, such as ZB bank's potential limitations on sharing sensitive information related to their fraud control measures. The study relied on self-reported data and information provided by banking institutions, which carried a risk of bias due to factors like information asymmetry, a lack of transparency in internal controls, or a desire to present a positive image. Consequently, the conclusions of the study may have been inaccurate or unreliable. The study may not have fully taken into account external factors that could influence fraud control measures, such as regulatory changes, socio-economic conditions, and technological advancements. These external factors could have impacted the effectiveness of fraud control measures but may not have been entirely accounted for in the study, potentially limiting the applicability of its findings and conclusions.

1.10 Definition of terms

Crime

Lombroso defined crime as "an act committed in violation of laws of a State which prescribe it, and which punish the act with penalties of loss of liberty or life" (Lombroso, 1876).

Fraud

The ACFE, a professional organisation dedicated to combating fraud, defines fraud as "any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means" (ACFE, 2018).

1.11 Summary

By providing a comprehensive overview of the research topic, problem statement, objectives, and limitations, Chapter 1 sets the stage for the subsequent chapters of the study. It establishes the context, justifies the importance of the research, and outlines the framework within which the study will be conducted. The next chapter focuses on the Literature Review of the study.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

This chapter will review literature in relation to fraud management in the banking systems of Zimbabwe and other countries. The chapter will unveil different theories in relation to fraud in banks, combating measures as suggested by other scholars a. It also includes the conceptual framework that guides the study, the summary of empirical studies, and the research gaps from various studies. Also, the chapter will be guided by the aforementioned research objectives.

2.1 The concept of fraud

Fungai Brian, (2014) defines fraud as consisting of four elements which are; false representation of material nature; knowledge that representation is false or reckless disregard of the truth; relevance entails that the person receiving the presentation reasonably and justifiably rely on it and damage being the financial loss. In Zimbabwe, Section 136 of the Criminal Law Codification and Reform Act 9:23 states that any person who makes a misrepresentation- (a) Intending to deceive another person or realising that there is a real risk or possibility of deceiving another person, and (b) Intending to cause another person to act upon the misrepresentation to his or her prejudice, or realising that there is real risk or possibility that another person may act upon the misrepresentation to his or her prejudice; shall be guilty of fraud if the misrepresentation causes prejudice to another person or creates real risk or possibility that another person may be prejudiced.

2.2 Theoretical framework

The theoretical framework for this study revolves around three main concepts: fraud, control measures and banking system of Zimbabwe. The integration and application of various theories related to fraud and fraud control will be scrutinised to provide a vivid understanding of the subject under study.

As pre-mentioned, the framework will include a number of theories including the agency theory, fraud triangle theory, fraud management theory and the diamond theory.

2.2.1 Agency theory

Agency theory, developed by Jensen and Meckling (1976), focuses on the relationship between principals (shareholders or owners) and agents (managers or employees) within an organisation. In the context of the banking system, agency theory helps explain the inherent conflicts of interest that arise between bank owners and employees, which can lead to fraudulent activities. The theory assumes that agents may act in their own self-interest, deviating from the principal's objectives and engaging in fraudulent behaviour to maximise personal gains. In an agency, there is a relationship between the appointer (principal) and an appointee (agent) who is expected to act on behalf of his/her appointer on different matters. An agency relationship will arise when one or more people employ another(s) to provide a service and even delegate the decision-making authority to him or her. The agent has a responsibility to optimise the benefits of the principal as well as have an interest in maximising his welfare (Soelton, 2020).

Agency theory describes firms as a structural necessity in the maintenance of contracts and controls in the firms to reduce the chances of the agents taking advantage of the principal. The management as the agents may face a dilemma on how they would their own interest without necessarily going against the business owners'. The theory is also used to analyse cooperating behaviour of the economic actors in order to achieve organisational goals. The dilemma for the agent is whether to maximise his own benefits or to work towards maximising his own personal interest and that of the organisation (Nwofia, 2018). Agency theory has been found to deal with the conflict between the principal and the agent, the agency costs and the interests of the principal and agent. While agency theory provides valuable insights into fraud management in the banking system, it is not without limitations. One limitation is the assumption that agents are solely motivated by self-interest. In reality, employees may have other motivations, such as job satisfaction or professional ethics, which can influence their behaviour. Additionally, agency theory does not account for the complexity of human behaviour and the potential for collusion among agents, which can lead to sophisticated fraud schemes. Therefore, the theory should be expanded to address the motivation behind the behaviours of the principal and agent, the principal's and agent's attitude towards risk besides time preference (Nyakarimi, 2020)

2.2.2 Principal-Agent Relationship in the Banking System

The banking system is characterised by a separation of ownership and control, where shareholders (principals) delegate decision-making authority to managers (agents) to run the bank's operations. This separation creates a potential conflict of interest between the shareholders' desire for profit maximisation and the managers' pursuit of personal goals (Jensen & Meckling, 1976). The agency theory provides a framework to analyse and mitigate these principal-agent problems.

Incentive Alignment and Risk-Taking Behavior

One of the key issues in the banking system is the misalignment of incentives between shareholders and managers. Managers may be tempted to take excessive risks to maximise their own short-term gains, while shareholders bear the long-term consequences of these actions. The agency theory suggests that aligning the interests of managers with those of shareholders through appropriate incentive structures can help mitigate this problem (Fama & Jensen, 1983).

Monitoring and Governance Mechanisms

The agency theory emphasises the importance of monitoring and governance mechanisms to reduce agency costs and ensure the alignment of interests. In the banking system, these mechanisms include board oversight, internal controls, and external audits. Effective monitoring can help detect and prevent opportunistic behavior by managers, thereby reducing the agency costs associated with information asymmetry (Jian, 2024).

Regulatory Implications

The agency theory also has significant implications for banking regulations. Regulators play the role of principals, aiming to protect the interests of depositors and maintain financial stability. By understanding the principal-agent problems inherent in the banking system, regulators can design regulations that align the interests of banks and their agents with those of society as a whole. For instance, capital adequacy requirements and risk-based supervision are regulatory measures to reduce agency costs and ensure the banking system's stability (Demirgüç-Kunt & Huizinga, 2010).

2.2.3 Fraud Triangle Theory

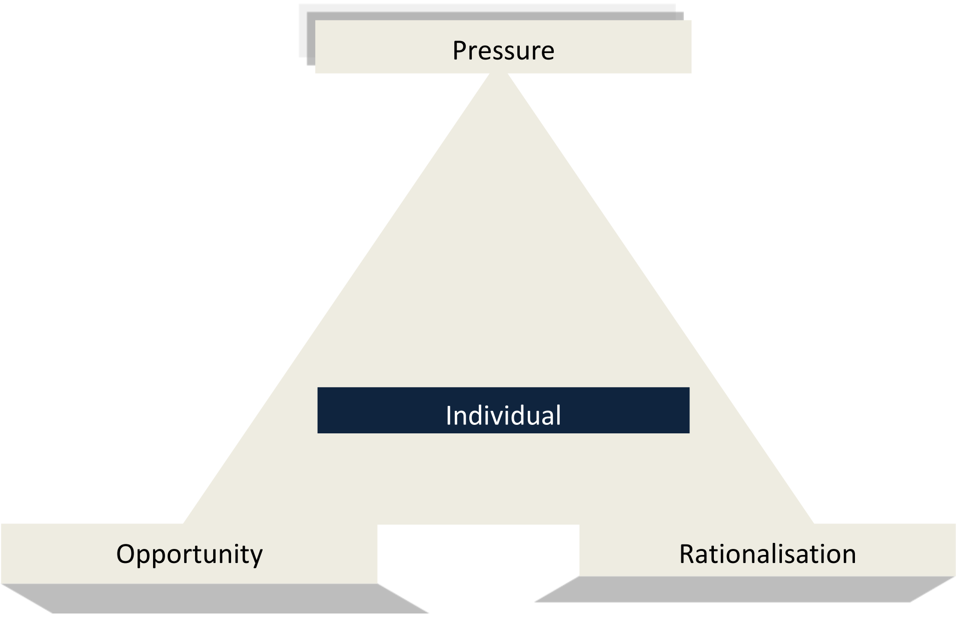


Figure 2.1: Fraud Triangle (Adopted from Cressey, 1973)

The fraud triangle theory, developed by Donald Cressey in 1973, identifies three essential factors that contribute to fraudulent behavior: perceived pressure, opportunity, and rationalization. According to this theory, fraud cannot occur without the presence of these three elements, and the severity of the fraud is determined by the strength of these factors(Nyakarimi, 2020). The theory suggests that a fraudster must have a motive or incentive to commit fraud, which can vary depending on the individual and may be driven by circumstances or a perceived lack of something important (Akelola, 2012).

Understanding the fraud triangle theory is crucial for the banking industry to develop effective strategies to prevent and detect fraudulent activities. By recognising the interplay between opportunity, rationalisation, and pressure, banks can implement preventive measures that address each element of the fraud triangle. For example, to reduce opportunities for fraud, banks must invest in robust internal controls and risk management systems. Recent citations by Shoetan et al. (2024) emphasise the importance of implementing advanced technologies, such as data analytics and artificial intelligence, to identify suspicious patterns and anomalies in financial transactions. Additionally, regular audits and independent reviews can help identify internal control weaknesses and ensure continuous improvement.

According to the fraud triangle theory, the presence of opportunity can tempt an individual to engage in fraudulent behavior. Opportunities to commit fraud often arise when employees identify weaknesses in internal controls, such as inadequate enforcement of rules and regulations, lack of segregation of duties, unclear guidelines and policies, and poor implementation of policies (Baba, 2019). These weaknesses create an environment where fraud can be committed without detection or consequences (Nyakarimi, 2020). The motivation to commit fraud cannot be acted upon without the presence of opportunity. Opportunities for fraud are created when employees violate policies, rules, and procedures, or when there is negligence or a lack of effective punishment for fraudulent behavior (Kulmie, 2023).

More so, creating an ethical culture within the banking industry is essential to combat rationalisation. Banks should prioritise ethical training programs that emphasise the consequences of fraudulent behavior and promote a strong corporate culture that encourages employees to report suspicious activities. Recent studies by Albrecht et al. (2019) highlight the positive impact of ethical training on reducing fraud incidents and fostering a culture of integrity within organisations. In brief, the fraud triangle theory provides a valuable framework for understanding the factors that contribute to fraudulent behavior within the banking system. By recognising the interplay between opportunity, rationalisation, and pressure, banks can implement preventive measures that address each element of the fraud triangle. Strengthening internal controls, promoting an ethical culture, and addressing financial pressures are essential steps in combating fraud within the banking industry. By adopting these measures, banks can safeguard their reputation, protect their customers, and contribute to the global financial system's stability. This theory is therefore relevant to the study as it establishes those reasons that may push a person to commit fraud. Based on the analysis of the factors that create environment for people to engage in fraudulent activities, those areas of the organisation’s regulations or actions that create opportunities to commit fraud and the reasoning that justifies employees' dishonest behaviour, the organisation can establish proper mechanisms that would effectively address the employees' concerns and reduce cases of frauds.

2.2.4 Fraud Diamond Theory

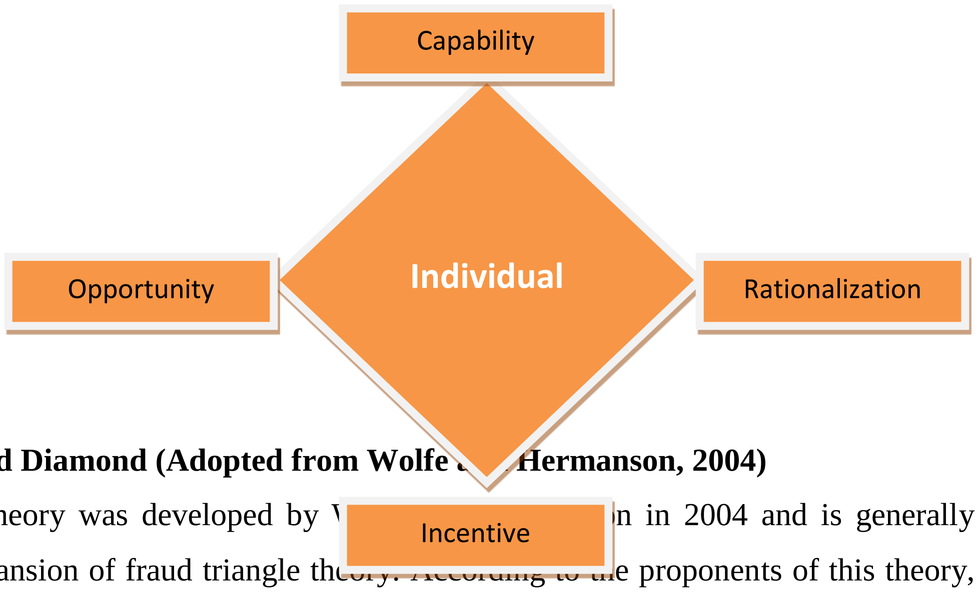


Figure 2.2: Fraud Diamond (Adopted from Wolfe [illegible] Hermanson, 2004)

Fraud diamond theory was developed by W[illegible]n in 2004 and is generally viewed as an expansion of fraud triangle theory. According to the proponents of this theory, the fraud triangle has been useful to accountants seeking to understand and manage fraud. However, it was necessary to enhance the theory by introducing the individual's capability (Wolfe & Hermanson, 2004). In their study, Abdullahi, Muhammad and Nuhu (2015) stated that though incentive, opportunity and a rationalisation to commit fraud may exist or coexist, it is difficult for fraud to be committed unless there is capability to do so. Fraud diamond theory states that, presence of opportunity, motive and rationalisation does not guarantee the occurrence of fraud. Wolfe and Hermanson (2004) stated that capabilities are personal traits and abilities that may play a role in whether the fraud will be committed or not even in the presence of incentive, opportunity and rationalisation. The capability to commit fraud is vital for the fraud to be perpetrated. The proponents of the theory listed four elements of capability. These elements include: first, the rank or duties of a person within the organisation may present chance to create or exploit an opportunity to commit fraud. Secondly, the right person to commit fraud must be smart or intelligent. The person must understand the weaknesses of the internal controls and has the capability to exploit these weaknesses (Abdullahi et al, 2015).

Thirdly the right person must have a lot of confidence that he will not be caught or detected and egocentric. The person believes that he can talk himself out of trouble easily. The fourth element of capability is presented as ability to force other employees to commit or hide fraud. Such a person can persuade others to convince others to commit fraud or to ignore the fraud (Wolfe & Hermanson, 2004). Wolfe and Hermanson (2004), indicated that most of multibillion dollar frauds would not have been committed if there were no people with right capabilities and in the right position. The theory has been used in the study as it is an enhancement of fraud triangle theory by including capability. Kassem and Ligson (2012) stated that though capability was added to fraud triangle theory to enhance it, unobservable elements of pressure and rationalisation should be replaced with integrity and motivation to form a new model. This theory is relevant as it may assist the management to put controls and measures in place to counter any fraudulent activity from those who may be in a position of influence.

2.3 FRAUD CONTROL MEASURES IN THE BANKING SYSTEMS

2.3.1 Know Your Client (KYC) Procedures

KYC procedures require banks to obtain and verify specific information about their clients, including their identity, address, and source of funds. By implementing robust customer identification processes, banks can significantly reduce the risk of fraud. According to a study by the International Monetary Fund (IMF), KYC measures have proven effective in preventing identity theft and impersonation, which are common techniques fraudsters use (IMF, 2016). By ensuring that customers are who they claim to be, banks can establish a strong foundation for trust and security. KYC also involves assessing the risk profile of customers to identify potential red flags and suspicious activities. Banks use various tools, such as transaction monitoring systems and risk scoring models, to detect unusual patterns or behaviours that may indicate fraudulent activities. These measures enable banks to take proactive steps in preventing fraud, such as freezing accounts or reporting suspicious transactions to regulatory authorities. A study by the Basel Committee on Banking Supervision found that KYC procedures significantly contribute to the early detection and prevention of fraud, reducing the financial losses incurred by banks (BCBS, 2014).

Furthermore, KYC is an effective tool for combating fraud and a legal requirement imposed by regulatory authorities worldwide. Banks must comply with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations, which necessitate implementing robust KYC procedures. Failure to comply with these regulations can result in severe penalties, reputational damage, and loss of business. Therefore, KYC acts as a deterrent for fraudsters, as they are more likely to target institutions with weaker compliance measures. However, while

KYC has proven to be effective in combating fraud, it is not without limitations and challenges. One of the main challenges is the increasing sophistication of fraud techniques, which can bypass traditional KYC measures. Fraudsters may use stolen identities or manipulate legitimate customer information, making it difficult for banks to detect fraudulent activities. Additionally, KYC procedures can be time-consuming and costly, potentially leading to customer dissatisfaction and increased operational expenses for banks.

2.3.2 Use of technology

Technological advancements have led to the implementation of robust security measures in the banking system, making it more difficult for fraudsters to exploit vulnerabilities. For instance, the introduction of biometric authentication methods, such as fingerprint and facial recognition, has significantly reduced the risk of identity theft and unauthorised access to accounts (Mlambo, 2019). These measures ensure that only authorised individuals can access their accounts, thereby minimising the potential for fraudulent activities. Technological development has enabled banks to implement real-time monitoring and detection systems, which can identify suspicious transactions and patterns. Advanced algorithms and artificial intelligence (AI) systems can analyse vast amounts of data, detecting anomalies and potential fraud attempts (Iavich, 2024). This proactive approach allows banks to take immediate action, preventing fraudulent activities before they cause significant damage. Technological development has facilitated the dissemination of information and improved customer awareness regarding fraud prevention. Banks can now provide educational resources, such as online tutorials and interactive platforms, to educate customers about common fraud schemes and precautionary measures (Mlambo, 2019). By empowering customers with knowledge, they become more vigilant and less susceptible to falling victim to fraudulent activities.

2.3.4 Regulatory frameworks

The regulatory framework of Zimbabwe's banking sector consists mainly of the Reserve Bank of Zimbabwe (RBZ) Act, the Banking Act, and various prudential guidelines and circulars issued by the central bank. These regulations primarily focus on enforcing capital adequacy, liquidity, and risk management requirements. However, the measures directed specifically towards combating banking fraud remain relatively limited. One of the key regulations addressing fraud is the Prevention of Corruption Act, which criminalises acts of bribery, corruption, and money laundering. Similarly, the Money Laundering and Proceeds of Crime Act is primarily concerned with money laundering and terrorist financing. While these legislations set the base for fraud prevention, they fail to sufficiently address the intricacies of fraud in the banking system.

The existing regulatory frameworks in Zimbabwe's banking system suffer from several notable loopholes, hindering effective fraud prevention and detection. First, a comprehensive definition of fraudulent activities within the banking sector is lacking. Identifying and prosecuting fraudsters without clear parameters becomes challenging, enabling fraudulent activities to persist.

Secondly, the coordination between regulatory bodies such as the RBZ, the Zimbabwe Anti-Corruption Commission (ZACC), and the Zimbabwe Republic Police (ZRP) needs improvement. Establishing better working relationships and information-sharing mechanisms among these entities is essential to efficiently combat banking fraud. Currently, the lack of collaboration and integration between these bodies results in fragmented enforcement and monitoring efforts. Furthermore, the current regulatory frameworks inadequately address the issue of internal fraud within banks. Internal fraud, perpetrated by employees or insiders, remains a significant concern. Consequently, establishing stringent regulations and monitoring mechanisms within banks is crucial to prevent such acts.

Therefore, several measures can be implemented to strengthen the fraud regulatory frameworks in Zimbabwe's banking system. First, a comprehensive definition of fraudulent activities should be established, encompassing various forms of fraud, including identity theft, cyber fraud, and corruption. Such a definition will aid in identification, investigation, and prosecution of fraudsters.

Secondly, there is a need for closer collaboration between regulatory bodies and law enforcement agencies. Joint task forces and regular information-sharing platforms must be created to expedite fraud investigations and bring culprits to justice. Additionally, the RBZ and other relevant bodies should regularly review and update prudential guidelines specific to fraud prevention. This will ensure that banks are well-prepared and equipped to detect and mitigate fraudulent activities. Lastly, creating a robust internal control and risk management framework within banks is crucial. Banks should employ independent internal audit departments and allocate adequate resources towards training employees on fraud awareness and prevention techniques. Additionally, stringent Anti-Money Laundering (AML) and Know Your Customer (KYC) measures must be implemented to safeguard against banking system infiltration and abuse.

2.4 CAUSES OF FRAUD INCIDENTS IN BANKING SYSTEMS

Fraud in the banking system is a complex issue with multifaceted causes. This literature review has highlighted several key factors contributing to fraud, including the lack of internal controls, technological vulnerabilities, organisational culture, and regulatory gaps. Addressing these causes requires a comprehensive approach that involves strengthening internal controls, investing in cybersecurity measures, fostering an ethical culture, and enhancing regulatory oversight. By understanding the underlying causes of fraud, policymakers, regulators, and banking institutions can work together to develop effective strategies to prevent and combat fraudulent activities, thereby safeguarding the integrity of the banking system.

2.4.1 Regulatory Gaps and Weak Enforcement

Political interference is one of the main causes of regulatory gaps and weak enforcement in Zimbabwe's banking system. Political elites exert their influence over regulatory bodies, compromising their ability to act independently and impartially. This interference hampers effective oversight, as political considerations often override the need for stringent regulatory frameworks and enforcement (MLambo, 2016). Another significant factor contributing to regulatory gaps is the outdated legislation governing the banking sector. For example, Zimbabwe has been operating with the Banking Act of 1965, failing to adequately address the complexities of modern banking and financial activities (Reserve Bank of Zimbabwe, 2016). This outdated legislation renders regulators inept in dealing with emerging challenges and fails to provide them with the necessary tools to oversee the sector effectively.

Also, according to Mlambo (2019) the banking sector of Zimbabwe faces constraints in terms of regulatory resources. Insufficient funding and lack of skilled personnel impede the ability of regulatory bodies, such as the Reserve Bank of Zimbabwe (RBZ), to enforce regulations effectively. Limited resources compromise the regulatory agencies' capability to carry out sufficient inspections, audits, and due diligence checks, resulting in weak enforcement and regulatory gaps. According to Chifamba (2019) to address regulatory gaps and weak enforcement, Zimbabwe must undertake comprehensive legislative reforms to update the current Banking Act. New legislation should address emerging challenge like technological advancements and evolving banking practices. Additionally, reforms should focus on granting regulators greater independence and authority to enforce regulations without political interference.

2.4.2 Lack of internal control system

Internal Control System in banks is important as the banks play a crucial and critical role in the development of the economy of a nation. The development in the economy can be hindered by macro-economic instabilities, corruption fraud and slowed real economic expansion. Strong and effective ICS in banks can address the aforementioned hindrances of economic development (Kumuthinidevi, 2016). ICS's effectiveness can be determined if, in the assessment of ICS components that include; control environment, risk assessment, control activities, communication of information, and monitoring are found to be present and working properly (COSO, 2013). An effective and efficient ICS will enable the organisations to operate without irregularities in that the financial statements produced will be of high quality. The effectiveness of ICS can be achieved if all the employees of the organisation can prioritise the organisation's interest above their own personal interests (Bangsa, 2018).

Literature has shown that the country's political environment is major causes of poor internal control systems. The political environment influences the appointment of key personnel within banks, often based on political affiliation rather than merit. This hampers the establishment of strong internal controls and promotes a culture of impunity, as individuals with political connections may exploit their positions for personal gains (ADB, 2018). For example, according to a report by the African Development Bank (2018), political interference in Zimbabwe's banking sector has resulted in the appointment of non-qualified or inexperienced individuals to key positions, compromising the effectiveness of internal control systems.

The shortage of skilled professionals in the banking sector also contributes to the absence of robust internal control systems. Due to economic challenges and brain drain, many talented individuals have left the country, leading to a scarcity of competent professionals capable of implementing effective control mechanisms (Chifamba, 2018). A study by the Zimbabwean Banking Association revealed a significant skills shortage within the banking industry, specifically in risk management, internal audit, and fraud prevention. This shortage impedes the establishment of a comprehensive internal control framework (ZBA, 2019). Also, the absence of a stringent regulatory framework exacerbates the lack of internal controls against fraud. Zimbabwe's banking sector has experienced gaps in legislation, enforcement, and supervision, which create an environment conducive to fraudulent activities (RBZ, 2018). A report by the African Development Bank (2017) highlighted the need for stronger regulatory oversight to combat fraud in the banking sector. The report emphasised the importance of updating legislation and increasing regulatory capacity to enhance internal control systems.

2.4.3Technological Vulnerabilities

The rapid advancement of technology has revolutionised the banking industry, but it has also introduced new avenues for fraud. Cybercriminals exploit vulnerabilities in banking systems, such as weak authentication protocols, malware attacks, and phishing scams, to gain unauthorised access to sensitive customer information or manipulate financial transactions. Studies have highlighted the importance of investing in robust cybersecurity measures to mitigate the risk of fraud in the digital age (Bhattacharya et al., 2018). In relation to Zimbabwe, Zimbabwean banks often neglect regular security updates on their systems, leaving them vulnerable to emerging threats and cyber-attacks. Many successful attacks exploit known vulnerabilities that could have been patched with the latest software updates. The absence of regular updates in the banking system increases the risk of fraud and compromises the integrity of the entire ecosystem (Symantec, 2020). A notable example showcasing the technological weaknesses in the Zimbabwean banking system is the 2019 case of CABS (Central Africa Building Society). A group of cybercriminals managed to compromise the bank's system and siphoned off over $3.6 million from various customer accounts (Chronicle, 2019). The breach occurred due to a combination of weak authentication methods and inadequate security measures, demonstrating the urgent need for stronger technological safeguards.

More so, a number of studies have shown that the absence of robust multi-factor authentication in online banking systems is a major factor promoting fraud activities (RBZ, 2021). MFA adds an extra layer of security by requiring users to provide multiple pieces of evidence to verify their identity, such as a password and a one-time passcode sent to their mobile device. As a result, by not implementing MFA, Zimbabwean banks are exposed to the risk of unauthorised access and potential fraud. However, the banking system in Zimbabwe also suffers from a technological weakness in the form of inadequate data encryption protocols (Symantec, 2020). Encryption is essential for securing sensitive data during transmission or storage. However, research conducted by cyber security firm, Symantec, indicates that a significant number of banks in Zimbabwe do not utilise strong encryption standards in their online banking applications (Symantec, 2020). This renders customer data susceptible to interception and unauthorised access.

2.4.4 Organisational Culture

African Development Bank (2018) also believes organisational culture within a bank plays a crucial role in shaping employee behavior and ethical standards. A toxic culture that prioritises short-term profits over ethical conduct can foster an environment conducive to fraudulent activities. Research has shown that a lack of ethical leadership, excessive pressure to meet unrealistic targets and a culture of silence contribute to the occurrence of fraud within banks (Cressey, 2019). Therefore, fostering a strong ethical culture and promoting transparency and accountability are essential in preventing fraud.

2.5 RESEARCH GAP

Fraud continues to be a significant concern in the global banking sector, posing risks to the stability and efficiency of financial systems. The Zimbabwean banking sector is no exception, facing persistent challenges related to fraud. Although there is existing literature on fraud in the banking sector, studies specifically addressing fraud control measures within the

Zimbabwean context, particularly with a dedicated focus on ZB Bank between 2020 and 2023, are limited. Furthermore, the identified research gap entails the need for an analysis of fraud control measures rather than general discussions on fraud occurrences. The specific examination of ZB Bank allows for a case study that provides insights into the effectiveness of fraud control measures employed by one of Zimbabwe's prominent banks.

2.6 CONCLUSION

The chapter has reviewed various literatures in relation to fraud, fraud controls and the banking system of Zimbabwe and its state in terms of fraud management systems. The chapter reviews related theories, exiting fraud control in the banking system of Zimbabwe. The literature above has shown that gaps still exist in relation to how Zimbabwean banking manages fraudulent activities.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

The aim of this chapter is to present the research methods that were used in the study. The chapter is divided into segments. The first section defines the research design concept. This is followed by the selection and justification of the research philosophy employed for the study. The third section will explain why employing the case study research approach was appropriate. The section on data collection describes the study population, sampling strategy and research instruments that were used. Finally, the chapter ends with a brief account on how data was analysed.

3.1 Research design

A research design refers to the master plan the research will follow. According to Jahoda, Deutch & Cook, ‘A research design is the arrangement of conditions for the collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy and procedure”. In this study, the researcher used a single case study design of ZB bank. Research design is the plan, structure and, strategy and investigation concaved so as to obtain ensured to search questions and control variance According to Yin (2003) he argues that one of the five rationales for a single case is when a case is representative or typical. As a result, ZB bank, one of the representatives of commercial banks in Zimbabwe, has been used as a case study and the results obtained will be applicable to other banks.

3.2 Research philosophy

According to Saunders et al (2009) there are different views about the way in which knowledge is developed. The two major philosophical schools of thought that have dominated the literature on the research process are positivism and phenomenology. Positivism (quantitative approach) Positivism as a philosophy adheres to the view that only "factual" knowledge gained through observation (the senses), including measurement, is trustworthy. In positivism studies, the role of the researcher is limited to data collection and interpretation through an objective approach and the research findings are usually observable and quantifiable. According to the principles of positivism, it depends on quantifiable observations that lead to statistical analysis. It has been noted that "as a philosophy, positivism is in accordance with the empiricist view that knowledge stems from human experience". It has an atomistic, ontological view of the world as compromising discrete, observable elements and events that interact in an observable, determined and regular manner", (Collins,2010). Phenomenological (qualitative approach) Creswell (2009) defined qualitative research as a means of exploring and understanding the meaning of individuals or groups ascribe to a social or human problem, and this means that the process involves emerging questions and procedures, data typically collected in the participants setting, data inductively building from particulars to general themes and the researcher making interpretations of the meaning of data. Hussey (1997) alluded that qualitative research (phenomenological approach) is subjective in its approach of examining and reflecting on perceptions of understanding social and human activities. In addition to that, Bryan (2004) echoed that the qualitative research approach embodies a view of social reality as a constantly shifting emergent property of individuals' creation. In carrying out the research, the researcher shared similar views with the above-mentioned authors, as the intention was to critically investigate and analyse specific research questions through the use of a qualitative approach.

3.3 Research Strategy

As outlined by Crewell (2013), various research strategies exist. However, given the study's nature, as explained in Chapter 1, the case study approach was deemed the most suitable methodology. According to Yin (2009), this approach is employed when investigating contemporary events that are beyond the researcher's control, seeking to answer "how" or "why" questions. In this study, the case study approach was used to explore how and why ZB Bank implemented its e-banking security strategies.

3.3.1 Advantages of case study

Apparently, there are a number of merits and demerits of using the case study approach. Data is examined within the natural setting of the investigation (Yin, 2003). Yin (1984) also noted that researchers should not confuse case studies with qualitative research. He emphasised that case studies can be based entirely on quantitative evidence. Block and Hosenfeld (1986) argued that variations in terms of intrinsic, instrumental and collective approaches to case studies allow for quantitative and qualitative data analysis. Punch (1998) has noted that case studies play a major role in training in business, law and medicine. He states that this is possible because cases are not totally unique. There is therefore transferability of knowledge from case to case.

3.3.2 Disadvantages of case study

Critics of the case study believe that, case studies fail to establish reliability or generality of findings. Some writers also say that the case approach can result in biased findings. Robert et al (2000) dismissed the view that case study research is only useful as an exploratory tool. Yet some researchers continue to use case study research method with successions carefully planned and crafted studies of real life 21 situations, issues, and problems. Yin (2003) has also pointed out that for case studies what is important is analytic and not statistical generalisation. Further, Punch (2000) states that if cases were not generalisable, they would not be used successfully in such the fields as law and medicine. It was against this background that this study employed the case study approach.

3.4 Population

According to Polit and Hungler (1999), a population is defined as the comprehensive collective of all individuals, entities, or members that share a common set of characteristics or criteria. In the context of this research, the population of interest comprised all management and staff members of ZB Bank.

3.5 Sampling Procedures

The study will employ a purposive sampling technique to select participants who possess relevant knowledge and experience in fraud control within the banking sector. According to Kelly (2010), purposive sampling is a method of selecting individuals expected to offer valuable and pertinent information to the research study. This study will target key stakeholders, including bank officials, auditors, and regulatory authorities. Utilising purposive sampling can enhance time efficiency and effectiveness by excluding individuals who lack knowledge about fraud, thereby enabling the researcher to concentrate on those who are more inclined to possess valuable information. This approach aids in saving time and streamlining the research process.

3.6 Sample Size

The sample size will consist of approximately 10 participants, including bank officials, auditors, and regulatory authorities. This sample size is considered adequate to understand the fraud control measures implemented by ZB Bank.

3.7 Data Collection Methods

Data collection will be done using designed semi-structured questionnaires. The questionnaires will consist of both open ended and closed-ended question. This type of research instrument will allow respondents to provide more detailed response and can provide deeper understanding of the study (Neuman, 2016).

3.8 Data Analysis Techniques

According to Neuman (2016), unlike quantitative research there is no standard format for analysing qualitative studies. In view of this, in the present study data was analysed in line with the recommendation of Miles and Hurberman (2014). In this research the qualitative data collected from interviews will be analysed using thematic analysis. This approach involves identifying recurring themes and patterns within the data. The quantitative data obtained from the research will be analysed using descriptive statistics, such as frequencies and percentages, to summarised the responses.

3.9 Research validity and Reliability

To ensure research validity and reliability, the study adopted suitable research design which is the blue print of the research. A case study research approach was used so as to answer the how' or 'why' questions about contemporary issues in relation to fraud control measures in the banking system of Zimbabwe. Also, appropriate semi-structured were used so as to allow participants to provide detailed responses in relation to the subject under study. More so, to ensure reliable responses, proper research ethics were followed. For example, participants were not threatened or forced to participate. Also, there were assured confidentiality of the responses they were going to provide.

3.10 Summary

This research methodology outlines the approach to be taken in assessing the fraud control measures implemented by ZB Bank in Zimbabwe from 2020 to 2023. By employing a mixed-method design, including interviews and surveys, the study aims to provide a comprehensive evaluation of the effectiveness of these measures. The research will critically analyse the strengths and weaknesses of the fraud control measures, contributing to the ongoing efforts to enhance fraud prevention in the Zimbabwean banking sector.

CHAPTER IV

RESULTS AND DISCUSSION

4.0 Introduction

This chapter is going to present and discuss the results found in the study. The presentation of the results will be guided by the research objectives. Thus, the presentation will be done in subsections based on the research objectives. Before diving into the results, the chapter will firstly describe the nature of the respondents used in the study.

4.1 Demographic characteristics of respondents

This section describes the characteristics of the respondents which participated in the study. Having this background help to validate the results of the study in terms of reliabilities and validity of responses gained from the study.

4.1.1 Gender ratio

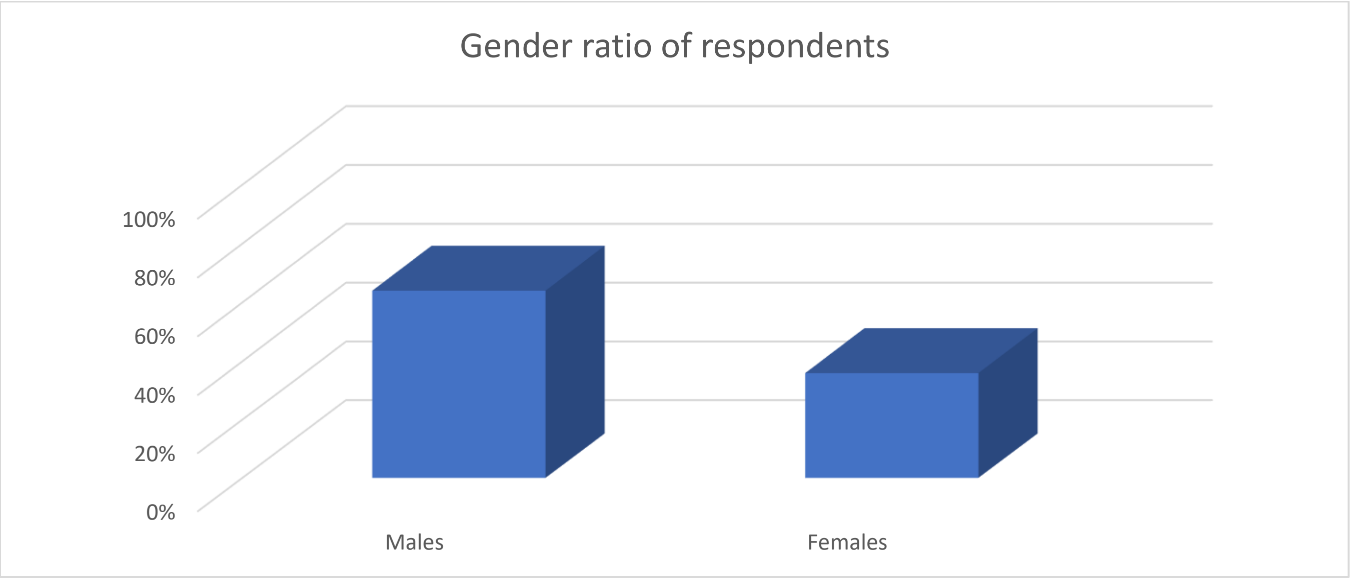


Figure 4. 1: Gender ratio of respondents

4.1.2 Age range of respondents

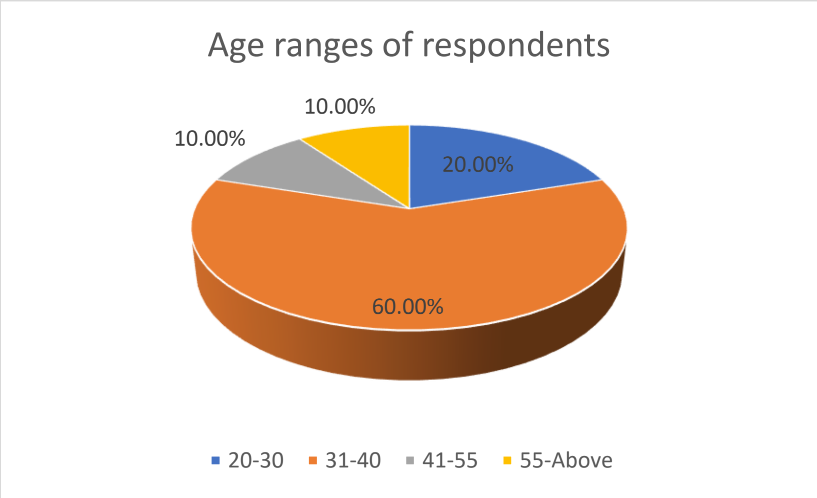


Figure 4. 2: Age range of respondents

4.1.3 Working experience

Table 4. 1: Working experience of respondents

Working Experience value	**Respondent**
1-5years]	30%
6-10 years	60%
11-15years	10%
20 years-Above	0%

4.2 Possible causes of fraud incidents in banking systems, specifically ZB bank

The responses from the respondents indicated that fraud is a result of many factors ranging from regulation, management and technological. The table below shows the results obtained from the study.

Table 4. 2: Possible motivating factors of fraud in the banking system

Factor	**No of respondents**	**Responses**	**Impact**	**Mean**	**St Dev**
Opportunity	N=10	7	0.28	4.166667	3.370625

Personal financial pressure	N=10	4	0.16	4.166667	3.370625
Greedy	N=10	2	0.08	4.166667	3.370625
Gambling	N=10	1	0.04	4.166667	3.370625
Corporate financial pressure	N=10	5	0.2	4.166667	3.370625
Others	N=10	6	0.24	4.166667	3.370625

Outcome indicate that most perpetrators commit fraud from opportunity rather than need supports the predator concept (Kranacher et al.,2011). Most responses from the respondents support the idea that fraudulent activities occur due to opportunities which include weak internal control, lack of regulations and fraud controlling framework as well as lack of improved technology.

According to Dorminey et al. (2010), in this representation, fraudsters seize opportunities to commit fraud without requiring rationalization or pressure, solely relying on the presence of an opportunity. This contradicts the fraud triangle theory, which suggests that individuals gradually succumb to fraud (Kranacher et al., 2011). However, it is important to note that this perspective may be limited, as it is based on observations rather than direct feedback from fraudsters themselves. Nevertheless, the study findings support the idea that non-shareable problems, such as financial pressures, social pressures, greed, and living beyond one's means, as identified by Cressey (2013), serve as motivators for fraudulent behavior.

4.3 To identify existing control measures implemented by ZB Bank

This section aimed at identifying existing measures or strategies being used by ZB bank in managing fraudulent activities. These factors were grouped into three category, namely strategic, operational and technological measures. The highest-rated factors were those with the highest frequencies.

4.3.1 Strategic factors

Table 4.3.1: strategic factors in fraud management

Factor	**Frequency (N=10)**	**Percentage**
Organisation learning for fraud prevention	6	60
Policy procedures	7	70
Use of historical data to predict fraud	7	70
Engaging consultants	6	60

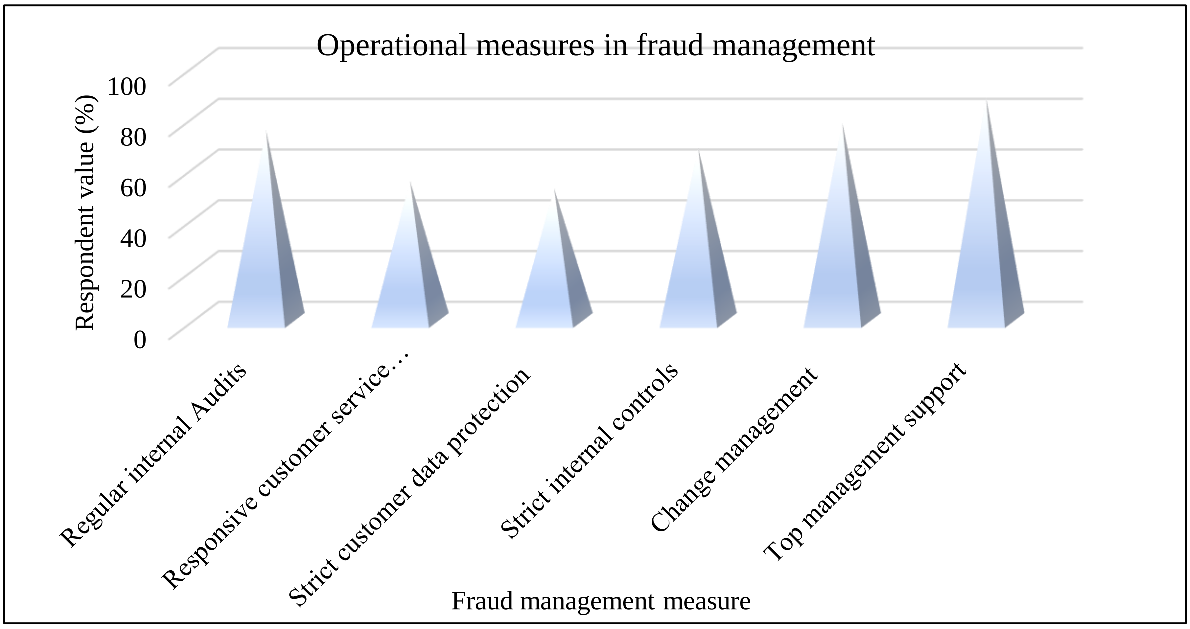
Consumer awareness	8	80

The highest rated factors from the strategic factor category were those related to banks being able to adapt and use available information to aid the decision-making process. The respondents felt that historical data to determine the probability of fraud was critical. This indicated the importance of banks not only storing data to meet retention requirements but also using it as a tool for intelligence. In contrast, using third parties to secure transactions obtained the lowest frequencies, which may suggest that respondents believed that banks should not heavily rely on external providers to secure their transactions.

4.3.2 Operational factors

Figure 4. 3: Operational factors in fraud management

Financial resources and top management support were the highest rated operational factors.



Interestingly, this does not relate to a specific measure or control that helps prevent fraud, but rather the commitment from management. It appears that the respondents take cognisance of fraud prevention as a continuous process requiring management commitment and financial resources to invest in people, technologies and processes. Customer data protection also rated highly indicating the importance of keeping customer data secure. Regular internal audits scored the lowest from the operational factor category indicating that other variables such as the internal controls that banks implement are more important than the frequency of which those controls are checked.

4.3.3 Technological measures

Table 4. 3.2: Technological factors in fraud management

Factor	**Frequency (N=10)**	**Percentage**
Two factor authentications	8	80
Real time fraud monitoring system	9	90
Biometric authentication	7	70
Data encryption	5	50

The study has shown that one of the most common technological measures used by ZB bank in fraud management is the implementation of two-factor authentication for online transactions. Two-factor authentication requires customers to provide two forms of identification before completing a transaction, typically a password and a unique code sent to their mobile device. This added layer of security helps to prevent unauthorised access to accounts and reduce the risk of fraudulent transactions. This can be supported by the study conducted by KPMG which found that two-factor authentication significantly reduces the risk of unauthorised access to online accounts, with 80% of banks reporting a decrease in fraud incidents after implementing this technology (KPMG, 2019). The study also found that customers have a higher level of trust in banks that use two-factor authentication, leading to increased customer retention and satisfaction.

Another technological measure used by ZB bank to combat fraud is the implementation of real-time fraud monitoring systems. These systems use artificial intelligence and machine learning algorithms to analyse transaction data in real-time, flagging any suspicious activity for further investigation. By detecting and preventing fraudulent transactions as they occur, banks can minimise their financial losses and protect their customers from potential harm. A study conducted by Deloitte found that real-time fraud monitoring systems can help banks save millions of dollars in fraud losses annually, with some banks reporting a 50% decrease in fraudulent transactions after implementing this technology (Deloitte, 2018). The study also found that customers have a higher level of trust in banks that use real-time fraud monitoring systems, leading to increased customer loyalty and retention.

The study also found that the bank uses biometric authentication technology to enhance security and combat fraud. Biometric authentication uses unique physical characteristics such as fingerprints or facial recognition to verify a customer's identity, providing a more secure and convenient way to access accounts and complete transactions. This is also supported by a study conducted by Accenture found that biometric authentication technology is highly effective in preventing fraud, with 90% of banks reporting a decrease in fraudulent transactions after implementing this technology (Accenture, 2020). The study also found that customers prefer biometric authentication over traditional methods such as passwords or PINs, leading to increased customer satisfaction and loyalty.

4.4 Challenge faced by the bank in its fraud control system

This section is going to explain possible challenges faced by the banking system of Zimbabwe specifically ZB bank in managing fraud. The results will be in subsection with each section explain each challenge. Also, possible solutions will be suggested.

4.4.1 Lack of Advanced Technology

One of the primary challenges faced by ZB Bank in fraud management is the lack of advanced technology to detect and prevent fraudulent activities. According to a study conducted by PwC, advanced technologies such as artificial intelligence and machine learning are essential in identifying suspicious patterns and anomalies that could indicate fraud. However, ZB Bank may lack the resources to invest in such technologies, making it more susceptible to fraudulent activities. Therefore, ZB Bank should invest in advanced technologies such as artificial intelligence and machine learning to enhance its fraud detection capabilities. These technologies can analyse vast amounts of data in real-time to identify suspicious patterns and anomalies, enabling the bank to take timely action to prevent fraud.

4.4.2 Insider Threats

Insider threats pose a significant challenge to ZB Bank in fraud management. Employees with access to sensitive information and systems may misuse their privileges to commit fraud. According to a report by the Association of Certified Fraud Examiners, insider fraud accounts for a significant portion of financial losses for organisations. As a result, ZB Bank should implement robust internal controls to mitigate the risk of insider fraud. This includes regular audits and monitoring of employee activities, as well as strict access controls to limit unauthorised access to sensitive information and systems.

4.4.3 Cross-Border Transactions

Cross-border transactions present a unique challenge to ZB Bank in fraud management. With the increasing globalisation of the banking industry, criminals have found new ways to exploit loopholes in international transactions to commit fraud. ZB Bank must collaborate with other financial institutions and regulatory authorities to establish robust anti-fraud measures for cross-border transactions.

4.4.4 Lack of Training and Awareness

Another challenge faced by ZB Bank in fraud management is the lack of training and awareness among employees. According to a study by KPMG, a significant number of fraud cases are a result of human error or ignorance. ZB Bank must invest in ongoing training programs to educate employees about the latest fraud schemes and prevention techniques.

4.5 Chapter summary

The aim of the chapter was to present and discuss the results found in the study. The chapter has managed to present results as required by each objective. Thus, the preceding chapter will provide final conclusions and recommendations of the study.

CHAPTER 5

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 INTRODUCTION

This chapter provides a comprehensive overview of the entire project, summarising the key findings and conclusions drawn by the researcher. It emphasises the researcher's recommendations based on the findings related to fraud control measures in the banking sector.

5.1 Summary of the major findings

The study aimed to identify possible causes of fraud incidents in the banking system, specifically focusing on ZB Bank. The factors identified included opportunities, personal financial pressure, greed, gambling, corporate financial pressure, and other non-shareable problems. The findings indicated that fraud in the banking system is primarily motivated by opportunities rather than need, contradicting the fraud triangle theory. Additionally, the study identified strategic, operational, and technological control measures implemented by ZB Bank to manage fraudulent activities. The highest-rated strategic factors included organisation learning for fraud prevention, policy procedures, use of historical data to predict fraud, engaging consultants, and consumer awareness. Operational factors highlighted the importance of financial resources, top management support, and customer data protection. Technological measures included two-factor authentication, real-time fraud monitoring systems, biometric authentication, and data encryption. ZB Bank faces several challenges in managing fraud within its banking system. These challenges include a lack of advanced technology for fraud detection, insider threats, cross-border transactions, and a lack of training and awareness among employees. These challenges can undermine the bank's ability to prevent and detect fraudulent activities effectively.

5.2 Conclusion

The study suggests that opportunities, weak internal controls, lack of regulations, and inadequate fraud control frameworks contribute to fraud incidents in the banking system. Non-shareable problems such as financial pressures, social pressures, greed, and living beyond means were also identified as motivators. The findings emphasise the importance of strategic measures in fraud prevention, including organisation learning, policy procedures, historical data analysis, engaging consultants, and creating consumer awareness. These measures highlight the significance of utilising available information and adapting to mitigate fraud risks. The study highlights the importance of top management support, financial resources, and customer data protection in fraud management. Regular internal audits were rated lower compared to other operational factors, suggesting that the effectiveness of internal controls is prioritised over the frequency of audits. ZB Bank employs effective technological measures such as two-factor authentication, real-time fraud monitoring systems, biometric authentication, and data encryption. These measures enhance security, reduce the risk of fraudulent transactions, and increase customer trust and satisfaction.

5.3 Recommendations

5.3.1 Strengthen Internal Controls

ZB Bank should continuously review and enhance internal control mechanisms to address the identified opportunities for fraud. This includes implementing robust control frameworks, stringent regulations, and regular internal audits. ZB Bank should establish comprehensive control frameworks that outline the policies, procedures, and guidelines for preventing and detecting fraudulent activities. The control frameworks should include segregation of duties, authorisation processes, and clear lines of responsibility to ensure accountability and minimise the risk of fraud. By defining and implementing these control frameworks, the bank can create a structured and controlled environment that reduces the opportunities for fraud. ZB Bank should adhere to and comply with relevant regulatory requirements and guidelines set by the banking industry and regulatory authorities. These regulations often include specific measures for fraud prevention and detection. By following these regulations, the bank ensures that it meets industry standards and reduces the likelihood of non-compliance-related fraud. Internal audits play a vital role in evaluating the effectiveness of internal controls and identifying any weaknesses or vulnerabilities that could be exploited by fraudsters. ZB Bank should conduct regular and thorough internal audits to assess the adequacy of its control mechanisms, identify potential areas of improvement, and address any deficiencies promptly. Internal audits help ensure that control measures are functioning as intended and provide opportunities for continuous improvement.

5.3.2 Focus on Organization Learning

The bank should invest in ongoing training and development programs to improve employees' knowledge and awareness of fraud prevention strategies. This will enable them to adapt to evolving fraud techniques and effectively respond to potential threats. Fraudsters constantly adapt and develop new techniques to exploit vulnerabilities in banking systems. By providing ongoing training, ZB Bank ensures that its employees stay informed about emerging fraud trends, tactics, and technologies. This enables employees to recognise and respond effectively to evolving fraud schemes, reducing the bank's susceptibility to new threats. Training programs can equip employees with the necessary skills to detect suspicious activities and potential red flags indicating fraudulent behavior. Employees trained to identify unusual transaction patterns, irregular customer behavior, or signs of social engineering tactics can play a critical role in early fraud detection. Employees become an additional layer of defense against fraudulent activities by improving their fraud detection skills. Training programs foster a culture of vigilance and awareness throughout the organisation. When employees understand the importance of fraud prevention and their role in safeguarding the bank and its customers, they are more likely to be proactive in reporting suspicious activities and adhering to established control measures. This collective vigilance creates a stronger defence against potential fraud incidents. Training programs can emphasise the importance of ethical behaviour and integrity in the workplace. By instilling a strong ethical culture, employees are more likely to resist the temptations of engaging in fraudulent activities. Ethical conduct becomes a core value within the organisation, reducing the likelihood of internal fraud and promoting a trustworthy environment for customers.

5.3.3 Enhance Technological Solutions

ZB Bank should continue leveraging advanced technological measures such as two-factor authentication, real-time fraud monitoring systems, and biometric authentication. Regular updates and investments in emerging technologies should be made to stay ahead of fraudsters. Implementing two-factor authentication adds an extra layer of security to customer transactions and account access. By requiring users to provide two forms of authentication, such as a password and a unique code sent to their mobile device, the bank can significantly reduce the risk of unauthorised access and identity theft. Two-factor authentication makes it harder for fraudsters to impersonate customers or employees, providing an added level of protection. Real-time fraud monitoring systems use advanced algorithms and machine learning techniques to analyse transaction data in real-time. These systems can detect suspicious patterns, anomalies, or deviations from normal customer behavior. By continuously monitoring transactions, the bank can identify and flag potentially fraudulent activities promptly. Real-time fraud monitoring allows for immediate action to be taken, such as blocking suspicious transactions or contacting customers to verify their actions. Biometric authentication, such as fingerprint or facial recognition, provides a high level of security and accuracy in verifying the identity of individuals. By implementing biometric authentication methods, ZB Bank can enhance the authentication process for customers' accounts and transactions. Biometric data is unique to each individual, making it difficult for fraudsters to replicate or bypass this form of authentication.

5.3.4 Collaborate with Consultants

Engaging experienced fraud prevention consultants can provide valuable insights and best practices to strengthen the bank's control measures. Regular consultations and external audits can help identify vulnerabilities and implement effective countermeasures. Fraud prevention consultants bring specialised knowledge and expertise in the field of fraud prevention. They have experience working with various organisations and have a deep understanding of industry best practices. By collaborating with consultants, ZB Bank can gain valuable insights into emerging fraud trends, innovative prevention techniques, and effective control measures. The consultants can provide guidance on implementing robust fraud prevention strategies tailored to the specific needs and challenges of the bank. External consultants can conduct comprehensive reviews and assessments of the bank's existing control measures, processes, and systems. They can identify potential vulnerabilities, weaknesses, or gaps in the bank's fraud prevention framework that may have been overlooked internally. By conducting thorough audits and assessments, consultants can help the bank identify areas for improvement and implement appropriate countermeasures to mitigate the risk of fraud. External consultants bring an unbiased and objective perspective to the table. They can assess the bank's fraud prevention practices without any internal biases or preconceived notions. This objectivity allows them to provide honest feedback and recommendations for improvement. They can challenge existing practices, policies, and procedures, ensuring that the bank's fraud prevention efforts are continually reviewed and refined. Fraud prevention consultants can work closely with the bank's management and stakeholders to develop customised solutions that align with the bank's specific goals, risk appetite, and regulatory requirements. They can assist in designing and implementing tailored fraud prevention programs, policies, and training initiatives. Consultants can also provide guidance on integrating new technologies, implementing data analytics, and developing fraud risk management frameworks. Fraud prevention consultants have a strong understanding of compliance and regulatory standards in the banking industry. They can help ensure that the bank's fraud prevention practices adhere to relevant laws, regulations, and industry guidelines. By collaborating with consultants, ZB Bank can proactively address compliance-related issues and stay up to date with evolving regulatory requirements.

5.3.5 Customer Education and Awareness

ZB Bank should prioritise consumer awareness programs to educate customers about common fraud schemes, prevention measures, and reporting channels. This will empower customers to play an active role in safeguarding their accounts and transactions. Customer education and awareness programs are essential for ZB Bank to empower its customers and strengthen the overall fraud prevention strategy. Educating customers about common fraud schemes, such as phishing, identity theft, or social engineering, enhances their awareness and understanding of potential risks. By providing information on how fraudsters operate and the tactics they use, customers can recognise and avoid falling victim to fraudulent activities. Knowledge empowers customers to make informed decisions and take proactive measures to protect themselves against fraud. Customer education programs can educate customers about effective prevention measures they can take to safeguard their accounts and transactions. This includes guidance on creating strong and unique passwords, using two-factor authentication, regularly monitoring account activities, and being cautious of sharing sensitive information. By arming customers with preventive strategies, ZB Bank helps create a collective defense against fraud. It is crucial for customers to know how and where to report suspected fraudulent activities. Customer education programs should provide clear information on reporting channels within the bank, such as dedicated fraud hotlines or email addresses. Prompt reporting enables the bank to take immediate action to investigate and mitigate potential fraud incidents, protecting not only the individual customer but also the broader customer base. By prioritising customer education and awareness, ZB Bank demonstrates its commitment to customer protection and security. This builds trust and enhances customer loyalty. When customers perceive that the bank prioritises their security and provides the necessary tools and knowledge to combat fraud, they are more likely to remain loyal and continue using the bank's services. Regulatory authorities often emphasise the importance of customer education and awareness in fraud prevention. By implementing robust customer education programs, ZB Bank ensures compliance with regulatory expectations and demonstrates its commitment to meeting industry standards. This helps maintain a positive reputation and minimises the risk of regulatory penalties.

REFERENCES LIST

ACFE. (2018). Report to the Nations 2018: Global Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-thenations.pdf

African Development Bank. (2018). Report on Zimbabwe's Banking Sector.

Akelola, S. (2012). *Fraud in the banking industry: A case study of Kenya*. Nottingham Trent University (United Kingdom).

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2019). Fraud examination. Cengage Learning.

Baba, L. L. (2019). *Effectiveness of forensic accounting services in financial crime detection and prevention in selected Public organisations in Dar Es Salaam Tanzania* (Doctoral dissertation, Kampala International University, College of Economics & management.).

Bhattacharya, S., Gopalakrishnan, S., & Kishore, R. (2018). Cybersecurity investments in the banking and finance sector: A literature review. Journal of Information Privacy and Security, 14(1), 2-19.

Boyle, D. M., DeZoort, F. T., & Hermanson, D. R. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy*, *34*(6), 578-596.

Chidavaenzi (2013 November 18) News Day, retrieve from https://www.newsday.co.zw/2013/11/18/messengerjailed-fraud

Chiwanza, T. (2017). The State of Cybersecurity in Zimbabwe's Banking Sector. International Journal of Economic Research, 14(1), 139-149.

Chronicle. (2019). CBZ Hit by US$3,6m Fraud.

Cressey, D. R. (2019). Other people's money: A study in the social psychology of embezzlement. Routledge.

Demirgüç-Kunt, A., & Huizinga, H. (2010). Bank activity and funding strategies: The impact on risk and returns. Journal of Financial Economics, 98(3), 626-650.

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. Journal of Law and Economics, 26(2), 301-325.

Fungai Brian, G. (2014). Challenges of Internal Bank Fraud Policy. A Case Study of Commercial Banks in Harare Central Business District. *International Journal of Management Sciences and Business Research*.

Gwakwara, C., Mukonza, R. M., & Mlambo, D. N. (2023). Rethinking, Remodelling and Retooling the Role of Parliamentary Diplomacy in the Formulation and Execution of Foreign Policy in Zimbabwe (2000-2017). *Journal of African Foreign Affairs, 10*(1), 169.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305-360.

Jian, J., He, K., Liu, Y., & Sun, Y. (2024). Corporate social responsibility: opportunistic behavior under earnings management?. *Asia-Pacific Journal of Accounting & Economics*, *31*(2), 247-268.

KPMG (2016) a guide to Preventing Workplace [9] Fraud International Journal of Management Sciences and Business Research, 2014

Kulmie, D. A. (2023). Financial crimes in Somali public sector: Causes and consequences. *International Journal of Economics and Finance*, *15*(4), 1-18.

Iavich, M., Kuchukhidze, T., & Gagnidze, A. (2024). NOVEL POST-QUANTUM DIGITAL SIGNATURE USING VERKLE TREES AND LATTICES. *Scientific and practical cyber security journal*.

Levi, M. (2019). Regulating fraud in the banking sector: A critical review. Criminology & Criminal Justice, 19(1), 3-20.

Local Consulting Firm. (2020). Technological Infrastructure Survey in Zimbabwean Banks.

Lombroso, C. (1876). L'Uomo Delinquente, Milan: Hoepli (5th edition, Turin: Bocca).

Mackevičius, J., & Giriūnas, L. (2013). TRANSFORMATIONAL RESEARCH OF THE FRAUD TRIANGLE. Ekonomika, 92(4),

Mansor, N., & Abdullahi, R. (2015). Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Science*, *1*(4), 38-45.

Mlambo, K., & Masiyandima, N. (2019). Corporate Governance Factors, Capital Regulation and Bank Risk Taking in Zimbabwe. *Business and Management Research*, *8*(3), 39-52.

Muradzikwa. G. (2013 April 19) Fraudulent claims on the increase: Zimbabwe independent, retrieved from, http://www.theindependent.co.zw/2013/04/19/fraudulent-claims-on-the-increase-muradzikwa/

Mutepfa, N.S. (2019). The role of the Reserve Bank of Zimbabwe in combating money laundering and terrorist financing. Journal of Money Laundering Control, 22(3), 399-414.

Nwofia, J. E. (2018). Contracting out services in the nigerian local government: implications for internal revenue generation. *Int'l J. Soc. Sci. Stud.*, *6*, 71.

Nyakarimi, S. N. (2020). *Internal Control System and Fraud Prevention in Banking Sector in Kenya* (Doctoral dissertation, University of Embu).

Reserve Bank of Zimbabwe (2017). Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) Guidance Notes for Banks. Retrieved from https://www.rbz.co.zw/uploads/aml_guidance_notes.pdf

Reserve Bank of Zimbabwe. (2017). Enhancing the Effectiveness of Regulatory Oversight and Supervision in Zimbabwe's Banking Sector.

Reserve Bank of Zimbabwe. (2021). Research Findings on the State of Bank Payment Systems in Zimbabwe. Retrieved from: [Insert URL]

Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. Journal of Finance, 52(2), 737-783.

Siddique, M., Islam, S. N., Hossain, M., Khatun, M., & Islam, M. R. (2018). Internal Control and Compliance of Banks. *Banking Review Series 2020*, 145.

Shoetan, P. O., Oyewole, A. T., Okoye, C. C., & Ofodile, O. C. (2024). Reviewing the role of big data analytics in financial fraud detection. *Finance & Accounting Research Journal*, *6*(3), 384-394.

Soelton, M., Ramli, Y., Anggraini, D., & Khosasi, D. (2020). Implementing Good Corporate Governance to Engage Corporate Social Rerponsibility in Financial Performance. *European Research Studies*, *23*(1), 239-258.

Symantec. (2020). Symantec SSL Labs.

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5). sage.

Zimbabwe Banking Association. (2019). Skills Gap in Zimbabwe's Financial Services Sector.

Zirima, H. (2015). Curbing Bank Fraud: The Role of Bank of Tanzania and Commonwealth Bank of Zimbabwe. International Journal of Accounting, Finance and Risk Management, 2(3), 140-148.

APPENDIX I:

LETTER OF INFORMED CONSENT

Dear Respondent.

My name is Natalia Lucia Musiyiwa (REG NO.: B202076B). I am a student at the Bindura University of Science Education studying towards a degree in Financial Intelligence. I am doing a research study entitled '**An assessment of fraud control measures in the Zimbabwean banking sector, case of ZB Bank for the period of (2020-2023)'.** Prior approval to conduct this study with the school as a case in point has been attained from the administration.

The researcher consequently requests you to voluntarily participate in this study and to be as honest as possible in answering the questions. Should you wish not to participate, then you should not respond to the questionnaire. The researcher wishes to assure you that your identity will not be revealed to any person(s) and your responses will be regarded as confidential. The information you provide will **not** be used outside its intended purpose.

In order to do justice to the said investigation, please complete the questionnaire to the best of your knowledge and ability. Please do not write your name on any part of the questionnaire. The questionnaire takes about ten minutes to complete.

Instructions

For your answers, you are kindly asked to tick in the box resembling your response or simply fill in the spaces provided.

Disclaimer: I hereby consent to participate in this research and I confirm that I have read the above information and agree with it.

Place: ………………………………….

Date: ………………………………….

Sign: ………………………………….

APPENDIX II

QUESTIONNAIRE GUIDE

SECTION 1:

Brief Background of the study

Fraud has become a significant concern for the banking sector worldwide, including Zimbabwe. As financial institutions strive to protect their customers and maintain the integrity of their operations, it is crucial to assess the effectiveness of fraud control measures. This study aims to evaluate the fraud control measures implemented by ZB Bank, one of Zimbabwe's leading financial institutions, during the period 2020-2023. By examining the bank's strategies, policies, and technologies, we can gain insights into the effectiveness of their fraud prevention efforts.

SECTION 2: Demographic section

Please Tick in the boxes where appropriate. *For example* ✓

2.1 The sex of the respondents

Male ☐ Female ☐

2.2 The a*ge range of respondent*

20-30 ☐ 31-40 ☐ 41-50 ☐ 51-Above ☐

SECTION 3: Professional section

3.1 Level of education

Diploma   Undergraduate degree   Master's degree   PHD

3.2 *Working Experience*

0-5 years ☐ 5-10 years ☐ 10-15 years ☐ 15years-Above ☐

3.3 *Working position:* ___

SECTION 4: **Fraud Control Policies and Procedures**

4.1 Does ZB Bank have a comprehensive fraud control policy in place?

Yes   No   Not sure

4.2 How frequently are these policies reviewed and updated?

Monthly   Quarterly   Annually   Not sure

4.3 Are employees regularly trained on fraud prevention techniques and policies?

Yes   No   Never

4.4 Are there specific procedures in place to detect and prevent fraud in different banking operations, such as online transactions, loan approvals, and account openings?

Yes   No   Not sure

If the above answer is yes, may you kindly explain the procedure below:

Section 5: Technology and Security Measures

5.1 What technological systems does ZB Bank utilise to detect and prevent fraud?

Yes   No   Not sure

If yes, may you please name or explain the system below:

5.2 Are there any specific software or tools used to monitor suspicious activities?

Yes | No | Not sure

If yes, may you please name or explain the system below:

5.3 Are there any measures in place to protect customer data and prevent unauthorised access?

Yes | No | Not sure

If yes, may you please name or explain the system below:

Section 6: Reporting and Investigation

6.1 How are suspected fraud cases reported within the bank? Please explain the steps below

6.2 Is there a designated department responsible for investigating fraud cases?

Yes	No	Not sure

If yes please name (or) and explain the characteristic of the department

6.3 Are employees encouraged to report any suspicious activities they come across?

Yes	No	Not sure

6.4 What actions are taken when a fraud case is confirmed? Please explain below

Section 7: Evaluation and Continuous Improvement

7.1 Are there any key performance indicators (KPIs) used to measure the effectiveness of these measures? Please name and explain below:

7.2 How does the bank incorporate feedback from employees and customers to improve fraud prevention strategies? Please explain below:

7.3 What challenges do you feel the banking is facing in improving or managing its fraud management system? Please explain or list the challenges below:

7.4 What measures do you feel the bank should put in place to improve its fraud management system? Please list or explain the measures below: