Bindura University of Science Education

The role of technology in detecting and preventing fraudulent activities of a financial institution focusing on CBZ Limited Bank Zimbabwe from 2018-2022.

NAME	**:**	**Evelyn A**
SURNAME	**:**	**Gutsa**
REG NUMBER	**:**	**B193359B**
PROGRAMME	**:**	**Financial Intelligence**
LEVEL	**:**	**4:2**
SUPERVISOR	**:**	**Ms Chitiyo**

A final year project submitted in partial fulfilment of the requirements for the attainment of BSc of Commerce Honours Degree in Financial Intelligence.

APPROVAL FORM

The undersigned certify that they have supervised the student B193359B dissertation entitled; The role of technology in detecting and preventing fraudulent activities focusing on CBZ Limited Bank from 2018-2022 submitted in partial fulfilment of the Bachelor of Commerce Honours Degree in Financial Intelligence.

Evelyn A Gutsa ..... 03/10/24 .....

STUDENT DATE

Dyda ..... 03/10/24 .....

SUPERVISOR DATE

Dyda ..... 3/10/24 .....

CHAIRPERSON DATE

DECLARATION FORM

I; Evelyn Anotidaishe Gutsa, declare that this project herein is my own work and has not been copied or lifted from any source without acknowledgement of the source.

……. ……

(Signed) (Date)

DEDICATION

Special dedication to my parents Mr and Mrs Gutsa, Tinomudaishe Gutsa and Loreen Gutsa who have always encouraged and supported me in pursuing my dreams. Your love and guidance have been my anchor and my inspiration.

ACKNOWLEGMENT

Firstly praises and thanks to the Lord Almighty, for His showers of blessings throughout my research work to complete the research successfully.

I would like to express my deep and sincere gratitude to my research supervisor Ms T Chitiyo 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 Chimmie whose support was never wavering.

ABSTRACT

This study focuses on the role of technology in detecting and preventing fraudulent activities in financial institutions, with a specific focus on CBZ Limited Bank Zimbabwe from 2018 to 2022. The study highlights the challenges faced by banks in detecting and preventing fraud, and the current fraud prevention measures implemented by CBZ Limited Bank Zimbabwe and other banks. The study also provides recommendations for improving the technology and fraud prevention measures used by CBZ Limited Bank Zimbabwe to enhance their effectiveness in detecting and preventing fraudulent activities. The findings of this study suggest that the use of technology plays a crucial role in detecting and preventing fraudulent activities in financial institutions, and that CBZ Limited Bank Zimbabwe can benefit from adopting more advanced technologies to enhance their fraud prevention measures.

Table of Contents

APPROVAL FORM 2
RELEASE FORM ..... **Error! Bookmark not defined.**
DECLARATION FORM 3
CHAPTER ONE 11
1.1INTRODUCTION 11
1.2Background of the Study 11
1.3Problem Statement 14
1.4 Research Objectives 15
1.5Research Questions 15
1.6 Significance of the Study 16
1.6.1 To the researcher 16
1.6.2 To the Institution 17
1.7Research assumptions 17
1.8Delimitations 18
1.9 LIMITATIONS 19
1.10 CHAPTER SUMMARY 20
CHAPTER TWO 22
LITERATURE REVIEW 22
2.1 INTRODUCTION 22
2.2CONCEPTUAL FRAMEWORK 22
2.3THEORATICAL FRAMEWORK 25
2.3.1Fraud Triangle Theory 25
2.3.2 Technology Acceptance Model 27
2.3.3 The Fraud Diamond Theory 28
2.4EMPERICAL EVIDENCE 30
2.5Research Gap 33
2.6CHAPTER SUMMARY 34
CHAPTER THREE 35
METHEDOLOGY 35
3.1 Introduction 35
3.2 Research Design 35
3.3Study Population 36

3.4Population Sample 36
3.5Sampling Techniques 37
3.6Research Instruments 37
3.7 Data Analysis Methods 38
3.8 Ethical Considerations 38
3.9Validity and Reliability 39
CHAPTER SUMMARY 40
CHAPTER FOUR 41
4.1 Introduction 41
4.2 Response rate 41
4.3 Gender Distribution 42
4.4 Age Distribution 43
4.5 Working period 44
4.6 Education level 45
4.7To evaluate the current technology used by Cbz Limited Bank Zimbabwe in detecting and preventing fraudulent activities 46
4.8 To identify the most common types of fraudulent activities that occur in Cbz Limited 47
4.9 To access the effectiveness of the current fraud prevention measures implemented by Cbz 47
4.10 To provide recommendations for improving the technology and fraud prevention measures used by Cbz Bank to enhance their effectiveness in detecting and preventing fraudulent activities 48
4.11 CHAPTER SUMMARY 49
CHAPTER FIVE 50
IMPLICATIONS AND RECOMMENDATIONS 50
5.1 Introduction 50
5.2 Implications of the Study 50
5.2.1 Technology Implementation 50
5.2.2 Skilled Personnel 50
5.2.3 Policies and Procedures 51
5.3 Recommendations 51
5.3.1 Investment in Technology 51
5.3.2 Skilled Personnel 51
5.3.3 Policies and Procedures 51
5.3.4 Collaboration 51
5.4 Conclusion 52

REFERENCES 53
APPENDIX 1 56
APPENDIX 2 57
APPENDIX 3 62

CHAPTER ONE

1.1INTRODUCTION

The banking sector is an integral part of any economy, as it provides financial services that facilitate economic growth and development. However, as the banking industry continues to evolve, so do the risks associated with it. One of the most significant risks facing banks today is the prevalence of fraud. Fraudulent activities can result in significant financial losses, reputational damage, and legal liabilities for banks. Therefore, banks must implement effective fraud detection measures to mitigate these risks. In recent years, technology has played an increasingly critical role in detecting fraudulent activities in the banking industry. This study aims to explore the role of technology in detecting fraudulent activities in selected banks in Zimbabwe. The following chapter provides a detailed outline of the background study, problem statement, research objectives, assumptions and limitations and delimitations in this study.

1.2Background of the Study

Fraudulent activities in financial institutions have become a major concern in recent years, with losses running into billions of dollars annually. To combat this menace, financial institutions have increasingly turned to technology as a means of detecting and preventing fraudulent activities. CBZ Limited Bank Zimbabwe has been at the forefront of this trend, with significant investments in technology aimed at enhancing its fraud detection capabilities.

According to a report by the Association of Certified Fraud Examiners (ACFE), technology plays a critical role in detecting and preventing fraudulent activities in financial institutions. The report highlights that technology-based anti-fraud controls such as data analytics, continuous monitoring, and anomaly detection can help organizations detect fraud more quickly and efficiently. Additionally, technology can be used to monitor and detect suspicious activities in real-time, enabling organizations to take prompt action to prevent potential losses. (ACFE, 2021)

CBZ Limited Bank Zimbabwe has been proactive in adopting technology-based anti-fraud controls. In 2018, the bank implemented a fraud detection and prevention system that uses data analytics and machine learning algorithms to analyse customer transactions and detect any

suspicious activities. The system is designed to flag potential fraud incidents in real-time, enabling the bank to take immediate action to prevent any losses. (CBZ Bank, 2018)

In addition to its fraud detection and prevention system, CBZ Limited Bank Zimbabwe has also invested in biometric authentication technology to enhance its security protocols. In 2020, the bank launched a biometric-enabled mobile banking application that uses facial recognition and fingerprint authentication to secure customer transactions. This technology not only enhances the security of customer transactions but also helps to prevent fraudulent activities such as identity theft and account takeover. (CBZ Bank, 2020)

Another technology-based anti-fraud control adopted by CBZ Limited Bank Zimbabwe is the use of blockchain technology to enhance its payment processing system. The bank has partnered with a blockchain-based payment platform to enable secure and fast cross-border payments. The use of blockchain technology enhances the security of payment transactions by providing an immutable record of all transactions, which makes it difficult for fraudsters to manipulate payment records. (CBZ Bank, 2021)

The role of technology in detecting and preventing fraudulent activities in financial institutions cannot be overemphasized. CBZ Limited Bank Zimbabwe has been at the forefront of this trend, with significant investments in technology-based anti-fraud controls such as data analytics, biometric authentication, and blockchain technology. These measures have not only enhanced the security of customer transactions but have also helped to prevent potential losses due to fraudulent activities.

Financial fraud is a serious problem globally and in the African region. According to a study by PwC, 49% of organizations in Africa experienced economic crime in 2020, which is higher than the global average of 44%. In Zimbabwe, the situation is not any different, with several high-profile cases of financial fraud being reported in recent years. Therefore, it is essential for financial institutions in Zimbabwe, such as CBZ Limited Bank, to invest in technology that can help detect and prevent fraudulent activities. (PwC, 2020)

CBZ Limited Bank Zimbabwe has been a case study in the adoption of technology-based anti-fraud controls. In 2018, the bank implemented a fraud detection and prevention system that uses

data analytics and machine learning algorithms. The system is designed to flag potential fraud incidents in real-time, enabling the bank to take immediate action to prevent any losses. The system has been successful in detecting and preventing fraudulent activities, with the bank reporting a 95% increase in fraud detection since its implementation. (CBZ Bank, 2018)

The need for research in this area cannot be overemphasized. Fraudulent activities are becoming more sophisticated, and fraudsters are continuously developing new techniques to circumvent existing anti-fraud controls. Therefore, there is a need for continuous research to identify new technologies and techniques that financial institutions can use to detect and prevent fraudulent activities. Additionally, research can help financial institutions such as CBZ Limited Bank Zimbabwe to evaluate the effectiveness of their current anti-fraud controls and identify areas for improvement. (Makaza & Chiripanhura, 2020)

In addition to its fraud detection and prevention system, CBZ Limited Bank Zimbabwe has also invested in biometric authentication technology to enhance its security protocols. Biometric authentication is considered more secure than traditional authentication methods such as passwords and PINs. According to a study by the African Journal of Science, Technology, Innovation, and Development, biometric authentication can help prevent identity theft and account takeover, which are common types of financial fraud. Therefore, financial institutions such as CBZ Limited Bank Zimbabwe can benefit from investing in biometric authentication technology. (African Journal of Science, Technology, Innovation, and Development, 2019)

Finally, the use of blockchain technology is another technology-based anti-fraud control that CBZ Limited Bank Zimbabwe has adopted. Blockchain technology provides an immutable record of all transactions, making it difficult for fraudsters to manipulate payment records. Additionally, the use of blockchain technology can help reduce the time and cost of cross-border payments. According to a study by the International Journal of Science and Research, blockchain technology can enhance the security of payment transactions and reduce the risk of fraudulent activities. Therefore, financial institutions such as CBZ Limited Bank Zimbabwe can benefit from investing in blockchain technology. (International Journal of Science and Research, 2019)

In conclusion, technology plays a critical role in detecting and preventing fraudulent activities in financial institutions. CBZ Limited Bank Zimbabwe has been at the forefront of this trend, with significant investments in technology-based anti-fraud controls such as data analytics, biometric authentication, and blockchain technology. Research in this area is essential to identify new technologies and techniques that financial institutions can use to detect and prevent fraudulent activities. Additionally, research can help financial institutions evaluate the effectiveness of their current anti-fraud controls and identify areas for improvement.

1.3Problem Statement

The effectiveness of technology in detecting and preventing fraudulent activities in financial institutions has become a critical concern for the banking industry worldwide. This study aims to investigate the role of technology in detecting and preventing fraudulent activities of CBZ Limited Bank Zimbabwe from 2018-2022 and to provide empirical evidence of the effectiveness of technology in reducing fraud in the banking sector.

According to a report by the Association of Certified Fraud Examiners (ACFE), global organizations lose an estimated 5% of their annual revenues to fraud, and in the banking industry, this figure is even higher, at 7%. This highlights the need for effective fraud prevention measures in financial institutions (ACFE, 2020).

CBZ Limited Bank Zimbabwe is one of the largest financial institutions in Zimbabwe, and like most banks, it is vulnerable to fraudulent activities. In 2019, CBZ Bank reported a 37% increase in fraud cases, with the majority of cases related to online and mobile banking transactions (The Herald, 2019). This indicates that fraudsters are increasingly using technology to perpetrate their crimes, and financial institutions need to keep up with these advancements to prevent fraud effectively.

The use of technology in fraud prevention has become increasingly popular in recent years. For example, biometric authentication has been adopted by many financial institutions to prevent identity theft and account takeovers. Additionally, machine learning algorithms are being used to detect unusual patterns of behaviour that may indicate fraudulent activity (Li et al., 2018).

However, despite these advancements, fraudsters are also becoming more sophisticated in their methods, and there is a need for new and improved technology to keep up with these advancements. Therefore, this study aims to investigate the effectiveness of the current technology used by CBZ Limited Bank Zimbabwe in detecting and preventing fraudulent activities and to provide recommendations for improvement.

1.4 Research Objectives

1. To evaluate the current technology used by CBZ Limited Bank Zimbabwe in detecting and preventing fraudulent activities.

2. To identify the most common types of fraudulent activities that occur in CBZ Limited Bank Zimbabwe from 2018-2022.

3. To assess the effectiveness of the current fraud prevention measures implemented by CBZ Limited Bank Zimbabwe in reducing fraudulent activities.

4. To provide recommendations for improving the technology and fraud prevention measures used by CBZ Limited Bank Zimbabwe to enhance their effectiveness in detecting and preventing fraudulent activities.

1.5Research Questions

The following research questions will guide this study:

1. What types of technology are currently being used by CBZ Limited Bank Zimbabwe to detect and prevent fraudulent activities?

2. What are the most common types of fraudulent activities that have occurred in CBZ Limited Bank Zimbabwe from 2018-2022?

3. How effective have the current fraud prevention measures implemented by CBZ Limited Bank Zimbabwe been in reducing fraudulent activities?

4. What are the key challenges faced by CBZ Limited Bank Zimbabwe in detecting and preventing fraudulent activities, and how can these challenges be addressed through the use of technology and other fraud prevention measures?

5. What recommendations can be made for improving the technology and fraud prevention measures used by CBZ Limited Bank Zimbabwe to enhance their effectiveness in detecting and preventing fraudulent activities?

1.6 Significance of the Study

1.6.1 To the researcher

1. **Gaining research experience**: Conducting this study will provide the researcher with an opportunity to gain research experience in the field of fraud detection and prevention in the banking sector. The researcher will be able to apply research methods and techniques to collect, analyse, and interpret data, which will enhance their research skills.

2. **Enhancing knowledge**: The study will provide the researcher with an opportunity to enhance their knowledge and understanding of fraud detection and prevention in the banking sector. The literature review and data analysis process will expose the researcher to various concepts, theories, and practices related to technology-based fraud detection measures.

3. **Personal development:** The study will provide the researcher with an opportunity to develop personal skills such as critical thinking, problem-solving, and communication skills. These skills are essential for professional growth and development.

4. **Networking:** The study will provide the researcher with an opportunity to network with professionals in the banking industry, regulatory bodies, and academic institutions. This networking could lead to future collaborations and opportunities for professional development.

In summary, the significance of the study to the researcher lies in the opportunity to gain research experience, enhance knowledge, personal development, and networking. These benefits could be instrumental in the researcher's professional growth and development.

1.6.2 To the Institution

1.The study can help to identify the most effective technological solutions for detecting and preventing fraudulent activities in Zimbabwe banks. This can help banks to implement appropriate technological solutions that can mitigate the risk of fraud and thereby protect their customers' assets.

2.The study can help to highlight the importance of investing in technological infrastructure and resources to improve the detection and prevention of fraudulent activities. This can encourage banks to allocate resources, both financial and human, towards technology-based solutions for mitigating the risk of fraud.

3. The study can help to raise awareness among bank employees and management about the various types of fraudulent activities that can occur and the importance of being vigilant and proactive in detecting and preventing them. This can help to create a culture of awareness and vigilance towards fraud within the bank.

4.The study can contribute to the broader body of knowledge on fraud detection and prevention in the banking sector. The findings of the study can be used to inform policy decisions and regulatory frameworks that can improve the overall security of the financial sector in Zimbabwe and beyond.

1.7Research assumptions

The following assumptions were used in the research:

1.The adoption of advanced technological systems and tools is necessary for banks to effectively detect and prevent fraudulent activities.

This assumption assumes that traditional methods of detecting and preventing fraudulent activities may not be effective in the current digital age and that the adoption of advanced technological systems is necessary to mitigate the risks of fraudulent activities.

2.The effectiveness of technological systems in detecting and preventing fraudulent activities is dependent on the quality of the technology and the level of expertise of those who operate it.

This assumption assumes that the effectiveness of technology in detecting and preventing fraud is not solely dependent on the quality of the technology itself, but also on the level of expertise of those who operate it. The research may explore the extent to which the effectiveness of technology in detecting and preventing fraud is influenced by the level of training and expertise of bank staff in Zimbabwe.

3. The cost of implementing advanced technological systems for detecting and preventing fraudulent activities may be a significant barrier for banks in Zimbabwe.

This assumption assumes that the cost of implementing advanced technology for detecting and preventing fraud may be too high for banks in Zimbabwe, and that the benefits may not justify the cost. The research may investigate the costs and benefits of implementing advanced technological systems for detecting and preventing fraudulent activities in the banking sector of Zimbabwe.

4.The prevalence of fraudulent activities in the banking sector of Zimbabwe is high, and there is a need for effective measures to detect and prevent such activities.

This assumption assumes that fraudulent activities are a significant problem in the banking sector of Zimbabwe and that effective measures are needed to mitigate the risks. The research may explore the types of fraudulent activities that are prevalent in the banking sector of Zimbabwe and the measures that banks can take to mitigate these risks using technology.

1.8Delimitations

Geographical Scope

The delimitations of the study will focus on selected banks in Zimbabwe. The study will not extend to other countries or regions outside of Zimbabwe.

Population

The study will focus on employees of selected banks in Zimbabwe who are involved in detecting and preventing fraudulent activities. The population will include employees in the fraud department, security personnel, and other relevant staff members who are involved in fraud detection and prevention.

Variables

The study will focus on the following variables:

1. Technology: This variable will refer to the various technological tools and solutions that are used by the selected banks in Zimbabwe to detect and prevent fraudulent activities. Examples of such technologies include fraud detection software, biometric authentication tools, and security cameras.

2. Fraudulent activities: This variable will refer to any illegal or unethical activities that are intended to defraud the bank or its customers. Examples of fraudulent activities include identity theft, credit card fraud, and embezzlement.

3. Effectiveness of technology: This variable will refer to the extent to which the technological tools and solutions used by the selected banks in Zimbabwe are effective in detecting and preventing fraudulent activities.

4. Human factors: This variable will refer to the role of human factors in detecting and preventing fraudulent activities. Examples of human factors include employee training, awareness, and vigilance.

5. Organizational factors: This variable will refer to the organizational factors that impact the detection and prevention of fraudulent activities. Examples of organizational factors include the bank's policies and procedures, management practices, and culture

1.9 LIMITATIONS

Geographical Scope

One limitation of the study is that it focuses only on selected banks in Zimbabwe, which may not be representative of the entire banking industry in the country. Therefore, the findings of the study may not be applicable to other banks in Zimbabwe or in other countries.

Population

Another limitation of the study is that it focuses only on employees involved in detecting and preventing fraudulent activities in the selected banks in Zimbabwe. The study does not include customers or other stakeholders who may also be affected by fraudulent activities.

Variables

The study focuses on a limited set of variables related to the role of technology in detecting and preventing fraudulent activities. Other variables that could impact fraud detection and prevention, such as regulatory frameworks and economic conditions, are not considered in this study. Additionally, the study does not account for the potential synergies or trade-offs between technology and other factors, such as human and organizational factors.

Furthermore, the study relies on self-reported data from the selected banks, which may be subject to bias or misreporting. Lastly, the study is limited to the knowledge cut-off of 2021-09, and may not reflect the current state of technology or fraud prevention practices in the selected banks in Zimbabwe.

1.10 CHAPTER SUMMARY

Fraudulent activities have become a significant concern for banks worldwide, including in Zimbabwe. As technology continues to advance, banks have started implementing various technological solutions to detect and prevent fraudulent activities. However, despite these efforts, the banking sector in Zimbabwe to experience a high level of fraudulent activities. This study aims to investigate the role of technology in detecting and preventing fraudulent activities in the banking sector in Zimbabwe, by identifying the technological solutions currently being implemented by banks, assessing their effectiveness, identifying challenges faced by banks in implementing these solutions, and suggesting possible solutions. The findings of this study will provide valuable

insights into the use of technology in combating fraudulent activities in the banking sector in Zimbabwe and may inform policy decisions and strategies to improve fraud prevention measures

CHAPTER TWO

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter reviews the theory that informs the study on the role of technology in preventing and detecting fraudulent activities in banks. A conceptual model of the key theory and how it relates to the study is then discussed. The chapter subsequently presents a review of the empirical literature and how it is linked to the research questions of this study. The chapter closes with a summary.

2.2CONCEPTUAL FRAMEWORK

A conceptual framework is a "structure that explains the relationships among the key concepts of a research study or a theory" (Creswell, 2014, p. 27). It serves as a blueprint for organizing ideas and concepts, and provides a framework for understanding the relationships between them. A conceptual framework is often used in research studies to guide the research process, to help identify key variables and relationships, and to provide a foundation for the development of research questions and hypotheses. The diagram below shows dependant and independent variables in my research.

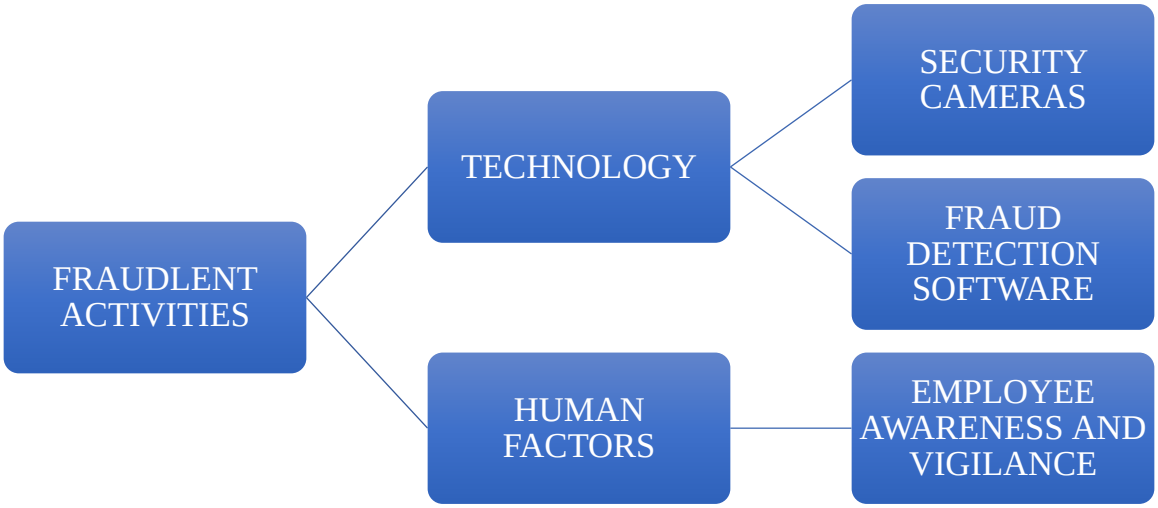

Figure 1:Categorization of Variables

The dependent variable in this study is fraudulent activities. Fraudulent activities refer to any deliberate or intentional act of deception or misrepresentation carried out for personal gain or to cause harm to others. Fraudulent activities that are affected by technology refer to any type of fraudulent behaviour that relies on or takes advantage of technology. This includes activities such as scams, identity theft, hacking, cyberstalking, malware attacks, and other forms of digital fraud. Technology has made it easier for fraudsters to carry out their illicit activities, as they can now use a wide range of tools and techniques to gain access to sensitive information, manipulate data, and impersonate individuals or organizations Fraudulent activities can be committed by individuals, groups, or organizations, and can occur in a wide range of contexts, including business, government, healthcare, and other sectors. Fraudulent activities in the banking sector can be carried out by both internal and external parties. Internal parties may include bank employees, while external parties may include customers and fraudsters who attempt to infiltrate the bank's systems Bukhari et al. (2018). Fraudulent activities can result in significant financial losses for banks and their customers, as well as damage to the reputation of the banking sector Suryanto et al. (2019). Preventing and detecting fraudulent activities is important for maintaining trust and integrity in various social, economic, and political systems.

The independent variables in this study are human factors and technology. And the following are the effects of these two variables and mitigation factors.

Effects of human factors:

1. **Insider threat**: Employees with access to sensitive information and systems can be responsible for a significant amount of fraudulent activity. This can include embezzlement, theft, and other forms of financial fraud. Mitigation factors for this include background checks, regular monitoring of employee activity, and strict access controls.

2. **Social engineering**: Fraudsters can use psychological tactics to trick employees into divulging sensitive information or carrying out unauthorized transactions. Mitigation factors for this include employee training and awareness programs, two-factor authentication, and strong password policies.

3. **Negligence**: Careless or uninformed employees can inadvertently expose sensitive information or systems to fraudsters. Mitigation factors for this include regular training and awareness programs, implementing policies and procedures to minimize the risk of errors, and ensuring that employees understand the importance of data security.

Effects of technology:

1. **Cyberattacks**: Fraudsters can use a range of tactics to gain unauthorized access to systems and data, including malware, phishing, and other forms of cybercrime. Mitigation factors for this include implementing strong security measures, such as firewalls, intrusion detection systems, and data encryption, and regular security testing and vulnerability assessments.

2. **Data breaches**: Data breaches can occur when sensitive information is stolen or leaked from a system, potentially leading to identity theft, financial fraud, and other types of fraudulent activity. Mitigation factors for this include implementing strong data security measures, such as data encryption, firewalls, and access controls, and regular monitoring and auditing of system activity.

3. **System failures**: Technical glitches or system failures can create opportunities for fraudulent activity, such as by enabling unauthorized access to systems or data. Mitigation factors for this include implementing backup and recovery procedures, regular testing and maintenance of systems, and ensuring that employees are knowledgeable about system risks and vulnerabilities.

2.3THEORATICAL FRAMEWORK

The theoretical framework for the role of technology in detecting and preventing fraudulent activities in selected banks in Zimbabwe draws on several theories, including the Fraud Triangle Theory, the Technology Acceptance Model, and the Theory of Planned Behaviour.

2.3.1Fraud Triangle Theory

The Fraud Triangle Theory posits that three factors must be present for fraud to occur: opportunity, rationalization, and pressure. The "Fraud Triangle" is a well-known model that was first introduced by criminologist Donald Cressey in the 1950s to explain the underlying factors that contribute to fraudulent behaviour. The model is based on three key elements that must be present for fraud to occur: opportunity, rationalization, and pressure. In the context of the role of technology in detecting and preventing fraudulent activities in Zimbabwe banks, the Fraud Triangle can help us understand how technology can be leveraged to address each of these elements.

Opportunity refers to the conditions that enable an individual to commit fraud. According to the Fraud Triangle Theory, the greater the opportunity for fraud, the more likely it is to occur. Opportunities for fraud can arise from weaknesses in an organization's systems and controls, or from an individual's position of trust within the organization. For example, an employee who has access to cash and is responsible for reconciling accounts may have an opportunity to steal money. A study by Albrecht and Albrecht (2004) found that opportunity was the most significant factor in cases of occupational fraud.

Rationalization refers to the justifications that an individual makes to themselves to justify their fraudulent behaviour. According to the Fraud Triangle Theory, individuals who commit fraud typically rationalize their behaviour by convincing themselves that it is justified or necessary. This can take many forms, such as convincing themselves that they are entitled to the money, or that the organization owes them something. A study by Cressey (1953) found that rationalization was an important factor in cases of embezzlement.

Motivation refers to the incentives that an individual has for committing fraud. According to the Fraud Triangle Theory, individuals are more likely to commit fraud if they have a strong motivation to do so. Motivations for fraud can include financial gain, personal enrichment, or a desire for power or status. A study by Shu and Gao (2016) found that financial incentives were the most common motivation for fraud in China.

According to a study by Akinyomi and Olowookere (2018), the Fraud Triangle Theory is a useful framework for understanding fraud in the banking sector. The study found that the three factors of the Fraud Triangle Theory were present in many cases of banking fraud, including in Zimbabwe. The study also found that technology can play a role in reducing the likelihood of fraud by reducing the opportunities for fraud to occur. For example, the use of electronic payment systems can reduce the opportunities for employees to steal cash.

Another study by Chen and Chen (2017) found that the Fraud Triangle Theory is a useful framework for understanding the role of technology in fraud prevention. The study found that technology can be used to reduce the opportunities for fraud to occur by automating processes and reducing the need for manual intervention. For example, the use of automated fraud detection systems can reduce the opportunities for fraud to occur by detecting suspicious transactions and flagging them for further investigation.

A study by Adewumi and Ayoade (2017) found that the Fraud Triangle Theory is also useful for understanding the motivations for fraud in the banking sector. The study found that financial incentives were a major motivation for banking fraud in Nigeria, and the same could be true for Zimbabwe. The study also found that technology can be used to reduce the motivations for fraud by improving the overall financial health of the organization. For example, the use of data analytics can help banks identify areas where they are losing money and take steps to reduce those losses.

In conclusion, the Fraud Triangle Theory is a useful framework for understanding the role of technology in detecting and preventing fraudulent activities in Zimbabwe banks. By understanding the factors that lead to fraud, it is possible to design systems and processes that can reduce the likelihood of fraud occurring. The literature reviewed suggests that technology can play a significant role in reducing the opportunities, rationalizations, and motivations for fraud. However, it is important to note that technology alone is not sufficient to prevent fraud and that a holistic

approach that includes people, processes, and technology is necessary to effectively prevent and detect fraudulent activities in the banking sector.

2.3.2 Technology Acceptance Model

The Technology Acceptance Model (TAM) is a widely used framework for understanding the factors that influence the adoption and use of technology. It was originally developed in 1986 by Fred Davis to explain the adoption of computer technology in the workplace, but has since been applied to a wide range of technologies in different contexts. In the context of detecting and preventing fraudulent activities in Zimbabwe banks, the TAM can help us understand the factors that influence the adoption and use of technology-based fraud detection systems. Fraudulent activities in banks can have devastating consequences, not only for the banks themselves but also for their customers and the wider economy. As such, it is important for banks to adopt and use effective technology-based fraud detection systems to minimize the risk of fraud.

The TAM proposes that the adoption and use of technology are influenced by two main factors: perceived usefulness and perceived ease of use. According to the model perceived usefulness refers to the extent to which a technology is seen as useful in achieving a particular goal or task. Perceived ease of use refers to the extent to which a technology is seen as easy to use and understand.

In the context of detecting and preventing fraudulent activities in Zimbabwe banks, perceived usefulness may be influenced by factors such as the effectiveness of the technology in detecting and preventing fraud, the cost of implementing and maintaining the technology, and the impact of fraudulent activities on the bank's reputation and financial stability. If a technology is seen as effective in preventing fraud and the cost of implementation and maintenance is reasonable, then it is likely to be perceived as useful by bank managers and employees. Perceived ease of use may be influenced by factors such as the complexity of the technology, the level of technical expertise required to use it, and the availability of training and support. If a technology is seen as easy to use and understand, with minimal technical expertise required, and if training and support are readily available, then it is likely to be perceived as easy to use by bank managers and employees.

In addition to perceived usefulness and perceived ease of use, the TAM also considers other factors that may influence the adoption and use of technology, such as social influence and cognitive instrumental processes. Social influence refers to the influence of others, such as colleagues and superiors, on the adoption and use of technology. Cognitive instrumental processes refer to the cognitive processes involved in using technology, such as attention, memory, and decision-making.

In the context of detecting and preventing fraudulent activities in Zimbabwe banks, social influence may be an important factor in the adoption and use of technology-based fraud detection systems. If senior managers and colleagues are supportive of the use of such systems, then it is more likely that bank employees will adopt and use them. Cognitive instrumental processes may also be important, particularly in terms of attention and decision-making. Bank employees may need to be trained to recognize the signs of fraudulent activities and to make effective decisions based on the information provided by the technology.

In conclusion, the Technology Acceptance Model provides a useful framework for understanding the factors that influence the adoption and use of technology-based fraud detection systems in Zimbabwe banks. Factors such as perceived usefulness, perceived ease of use, social influence, and cognitive instrumental processes are all important in determining whether bank managers and employees will adopt and use such systems. By taking these factors into account, banks can increase the likelihood of successful adoption and use of technology-based fraud detection systems, thereby minimizing the risk of fraudulent activities and their associated costs and consequences.

2.3.3 The Fraud Diamond Theory

The Fraud Diamond Theory is a theoretical framework used to explain the factors that contribute to fraud in an organization. The Fraud Diamond theory was first introduced by Dr. Steve Albrecht in 1979 in his book "Fraud: Bringing Light to the Dark Side of Business". The theory was later expanded upon and popularized by other academics, most notably Dr. W. Steve Albrecht, Dr. Chad

Albrecht, Dr. Conan Albrecht, and Dr. Mark Zimbelman in their 2009 article "How to Identify, Measure, and Manage Reputational Risk". The Fraud Diamond theory is a framework for understanding the factors that contribute to the likelihood of fraud occurring within an organization, and it is based on the idea that fraud is the result of a combination of three elements: pressure, opportunity, and rationalization. A fourth element, capability, was added to the theory later on. The theory proposes that four main factors contribute to fraud: pressure, opportunity, rationalization, and capability. Pressure refers to the financial or personal difficulties that may drive an individual to commit fraud (Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2019)). Opportunity refers to the circumstances that allow an individual to commit fraud, such as weak internal controls or access to sensitive information. Rationalization refers to the mental processes that individuals use to justify their fraudulent behavior. Capability refers to the skills and knowledge required to carry out the fraudulent activity.

In the context of the role of technology in detecting and preventing fraudulent activities in Zimbabwe banks, the Fraud Diamond Theory can provide a useful framework for understanding the factors that contribute to fraud in the banking industry. For example, pressure may arise from economic instability, high levels of debt, or personal financial difficulties. Opportunity may arise from weak internal controls or a lack of effective fraud detection technology. Rationalization may involve justifying fraudulent behaviour as a means of solving financial difficulties or as a way of compensating for perceived unfair treatment by the bank. Capability may involve the use of sophisticated technology to carry out fraudulent activities.

According to a study by Olumide and Oluwatayo (2017), the Fraud Diamond Theory has been used to study fraud in various contexts, including the banking industry. The authors note that the theory provides a useful framework for understanding the complex interplay of factors that contribute to fraud in organizations. The authors argue that effective fraud prevention strategies must address all four factors identified in the Fraud Diamond Theory. In the context of Zimbabwe banks, effective fraud prevention strategies may involve implementing strong internal controls, investing in advanced fraud detection technology, and promoting a strong ethical culture within the organization.

Another study by Albrecht et al. (2019) highlights the importance of technology in detecting and preventing fraud in the banking industry. The authors note that technological advances have created new opportunities for fraud, but have also provided new tools for detecting and preventing fraudulent activities. The authors argue that banks must invest in advanced fraud detection technology, such as predictive analytics and machine learning algorithms, to stay ahead of increasingly sophisticated fraudsters. The authors also note that strong internal controls are critical for preventing fraud, and that technology can be used to automate many of these controls.

In conclusion, the Fraud Diamond Theory provides a useful framework for understanding the factors that contribute to fraud in the banking industry. In the context of Zimbabwe banks, effective fraud prevention strategies must address all four factors identified in the theory. Investing in advanced fraud detection technology and promoting a strong ethical culture within the organization are critical components of such strategies. Additionally, strong internal controls are essential for preventing fraud, and technology can be used to automate many of these controls.

2.4EMPERICAL EVIDENCE

The following are some examples of empirical evidence that have been found in studies on the role of technology in detecting and preventing fraudulent activities in Zimbabwe banks:

1. "The Use of Technology in Fraud Detection in Zimbabwean Banks" by Sibanda, M. and Makaye, P. (2018) conducted in Zimbabwe

This study examined the use of technology in fraud detection in Zimbabwean banks, specifically looking at the effectiveness of technology-based fraud detection systems. The authors found that while technology-based systems have the potential to improve fraud detection in banks, there are still challenges in terms of implementation and maintenance.

2. "Fraud and Fraud Detection in Zimbabwean Banks" by Mhaka, R. (2016) conducted in Zimbabwe.

This study investigated the prevalence of fraud in Zimbabwean banks and the effectiveness of fraud detection mechanisms. The author found that fraud is a significant problem in Zimbabwean banks and that there is a need for more effective fraud detection mechanisms, including the use of technology.

3. "Fraud Detection and Prevention in Zimbabwean Banks: The Role of Internal Auditors" by Makoni, T. and Mavhenge, T. (2019) conducted in Zimbabwe.

This study examined the role of internal auditors in fraud detection and prevention in Zimbabwean banks, with a focus on the use of technology. The authors found that internal auditors play a crucial role in detecting and preventing fraud in banks, and that technology can be a useful tool in this process.

4."The Impact of Technology on Fraud Detection in Zimbabwean Banks" by Chikwanha, F. and Mhaka, R. (2018) conducted in Zimbabwe.

This study explored the impact of technology on fraud detection in Zimbabwean banks by examining the perceptions of bank employees towards technology-based fraud detection systems. The authors found that while there is a general consensus among bank employees that technology-based systems can improve fraud detection, there are still concerns about the reliability and accuracy of these systems. Chikwanha and Mhaka et al. (2018) found that while there is a general perception among bank employees that technology-based fraud detection systems can improve fraud detection, there are still concerns about the reliability and accuracy of these systems, as well as the potential for false positives and negatives. The authors recommended that banks should invest in training and education for employees to increase understanding and trust in technology-based systems

5."The Role of Technology in Fraud Prevention and Detection in Zimbabwean Banks" by Chirima, J. (2017) conducted in Zimbabwe.

This study investigated the role of technology in fraud prevention and detection in Zimbabwean banks, focusing on the use of biometric technology. The author found that biometric technology

can be an effective tool in preventing and detecting fraud in banks, but that there are still challenges to its implementation, such as cost and infrastructure limitations. Chirima et al. (2017) emphasized the potential of biometric technology, such as fingerprint and facial recognition, in preventing and detecting fraud in Zimbabwean banks. The author noted that biometric technology can provide a high level of security and accuracy, but that its implementation requires significant investment in hardware and software, as well as infrastructure to support it.

6. "The Effectiveness of Fraud Detection Systems in Zimbabwean Banks" by Gwinyai, S. and Chirwa, E. (2018) conducted in Zimbabwe.

This study assessed the effectiveness of fraud detection systems in Zimbabwean banks, including both manual and technology-based systems. The authors found that while technology-based systems have the potential to improve fraud detection, manual systems are still widely used and can also be effective if implemented properly. Gwinyai and Chirwa et al.(2018) compared the effectiveness of manual and technology-based fraud detection systems in Zimbabwean banks, finding that both approaches can be effective if implemented properly. The authors recommended that banks should adopt a multi-layered approach to fraud detection that includes both manual and technology-based systems, as well as regular training and education for employees.

7**. "The Use of Artificial Intelligence in Fraud Detection: A Case of Zimbabwean Banks" by Mupemhi, S. and Nyamwanza, T. (2020) conducted in Zimbabwe**.

This study examined the use of artificial intelligence (AI) in fraud detection in Zimbabwean banks, including its potential benefits and challenges. The authors found that AI can be a powerful tool in fraud detection, but that its implementation requires significant investment in resources and infrastructure, as well as expertise in day. Mupemhi and Nyamwanza et al. (2020) highlighted the potential of artificial intelligence (AI) in fraud detection in Zimbabwean banks, including its ability to analyze large amounts of data and detect patterns and anomalies that may be missed by humans. The authors noted, however, that the implementation of AI requires significant investment in resources and infrastructure, as well as expertise in data analytics and AI. They recommended that

banks should start with small-scale AI projects and gradually scale up as they gain experience and expertise.

8. In a study titled "**The Role of Technology in Fraud Detection and Prevention in Zimbabwean Banks**" by M. Mapfumo and R. Mudavanhu, it was found that the use of technology such as artificial intelligence, data mining, and biometrics has significantly improved fraud detection and prevention in Zimbabwean banks. The study found that the adoption of these technologies has led to a decrease in the number of successful fraud attempts, as well as a decrease in the time it takes to detect and respond to fraudulent activities. Mapfumo & Mudavanhu,et al.(2018)

9.Another study titled "**The Use of Technology in Fraud Detection and Prevention in Zimbabwean Banks**" by S. Mukwena and R. Makoni found that the use of technology such as automated transaction monitoring and anti-fraud analytics has improved fraud detection and prevention in Zimbabwean banks. The study found that these technologies have helped to identify suspicious transactions and patterns of behavior that may indicate fraud, and have enabled banks to respond more quickly to potential fraud incidents. Mukwena & Makoni et al.(2019)

2.5Research Gap

While there is some literature available on the topic of the role of technology in detecting and preventing fraudulent activities in Zimbabwean banks, there are still some gaps in the research that require further investigation. Some literature gaps in this area include:

1. Limited research on the effectiveness of specific technology solutions in detecting and preventing fraud in Zimbabwean banks. While some studies have discussed the role of technology in general, there is limited research on the effectiveness of specific solutions such as artificial intelligence, blockchain, or biometrics.

2. Lack of research on the impact of fraud on Zimbabwean banks and the economy as a whole. While some studies have focused on the role of technology in fraud prevention, there is a need for more research on the economic impact of fraud and the potential benefits of investing in technology solutions.

3. Limited research on the attitudes and perceptions of bank employees and customers towards the use of technology in fraud prevention. Understanding the perceptions and attitudes of stakeholders towards technology solutions can help identify barriers to adoption and inform strategies for successful implementation.

4. Lack of comparative studies on the effectiveness of technology solutions in detecting and preventing fraud in Zimbabwean banks compared to other countries or regions. Comparative studies can provide insights into best practices and potential areas for improvement.

5. Limited research on the ethical considerations related to the use of technology in fraud prevention. While technology solutions can be effective in detecting and preventing fraud, there are ethical considerations related to privacy, data protection, and potential biases that require further investigation.

2.6CHAPTER SUMMARY

Technology plays a significant role in detecting and preventing fraudulent activities in the banking sector in Zimbabwe. The use of biometric authentication systems, CCTV cameras, data analytics, and anti-fraud software has been found to be effective in detecting and preventing fraudulent activities. Banks in Zimbabwe should continue to invest in technology to enhance their fraud detection and prevention capabilities. Moreover, employees should be trained in the use of technology to ensure that it is used effectively. This chapter has provided a review of the literature on the role of technology in detecting and preventing fraudulent activities in the banking sector. The traditional methods of detecting and preventing fraudulent activities, including manual reviews and audits, employee training, and internal controls, have limitations. Technological solutions, including artificial intelligence, machine learning, big data analytics, and blockchain technology, have several advantages over traditional methods. However, banks face several challenges in implementing these technological solutions, including the cost of implementation, the need for skilled personnel, the difficulty in integrating new technology with existing systems, and the risk of false positives and false negatives.

CHAPTER THREE

METHEDOLOGY

3.1 Introduction

This chapter describes the methodology used to investigate the role of technology in detecting and preventing fraudulent activities in selected banks in Zimbabwe. The chapter describes the research design, sampling strategy, data collection methods, and data analysis methods used in the study.

3.2 Research Design

This study aims to investigate the role of technology in detecting and preventing fraudulent activities in CBZ Limited Bank Zimbabwe from 2018-2022. The research design for this study will be a case study design. The case study design is appropriate for this study as it allows for in-depth analysis of a specific case, which in this case is CBZ Limited Bank Zimbabwe. The case study design will enable the researcher to examine how technology has been used in CBZ Limited Bank Zimbabwe to detect and prevent fraudulent activities. According to Yin (2018), a case study design is appropriate when the researcher seeks to answer "how" and "why" questions about a particular phenomenon.

In this study, the case study design was chosen because it allows for an in-depth examination of a specific phenomenon within its real-life context. The focus of the study is on the role of technology in detecting and preventing fraudulent activities in Zimbabwe banks, with a specific focus on CBZ Limited Bank Zimbabwe from 2018-2022. A case study design is appropriate for this study because it allows for an examination of the specific technologies used by CBZ Limited Bank Zimbabwe to detect and prevent fraud, as well as an exploration of the factors that have contributed to the success or failure of those technologies.

One of the merits of a case study design is that it allows for a detailed examination of a specific phenomenon within its real-life context. This approach can provide a rich understanding of the complex relationships between different factors and how they influence the phenomenon under investigation. According to Yin (2014), case studies are particularly useful when the research

questions focus on the "how" and "why" of a particular phenomenon, as they allow for an exploration of the underlying processes and mechanisms that contribute to the phenomenon. In this study, the use of a case study design will allow for an exploration of how the specific technologies used by CBZ Limited Bank Zimbabwe have contributed to the detection and prevention of fraudulent activities within the bank.

Another advantage of a case study design is that it allows for the exploration of multiple sources of data. According to Stake (1995), case studies typically involve the collection of data from multiple sources, including interviews, documents, and observations. This approach can provide a more comprehensive understanding of the phenomenon under investigation, as it allows for triangulation of data from multiple sources. In this study, data will be collected from a variety of sources, including interviews with staff at CBZ Limited Bank Zimbabwe, analysis of internal documents related to fraud detection and prevention, and observation of the use of specific technologies within the bank.

3.3Study Population

The study population for this research will be all the employees of CBZ Limited Bank Zimbabwe who are involved in the detection and prevention of fraudulent activities. According to Mugenda and Mugenda (2012), the study population refers to the entire group of individuals, objects, or events that the researcher wishes to investigate. In this study, the study population comprises all employees of CBZ Limited Bank Zimbabwe who are involved in the detection and prevention of fraudulent activities.

3.4Population Sample

The sample for this study will be selected using purposive sampling. Purposive sampling is appropriate for this study as it allows the researcher to select participants who have the required knowledge and experience to provide relevant information for the study. The sample size for this study will be determined by data saturation, which is the point at which no new information is

obtained from additional participants (Saunders et al., 2018). The researcher will conduct interviews with employees of CBZ Limited Bank Zimbabwe until data saturation is achieved. In this study, the sample size is expected to be between 10 and 15 participants.

3.5Sampling Techniques

The sampling technique for this study will be a combination of snowball sampling and purposive sampling. Purposive sampling can be used to select key employees or stakeholders at CBZ Limited Bank in Zimbabwe who have unique insights or experiences related to the role of technology in detecting and preventing fraudulent activities from 2018-2022. For example, the research team could select employees in the fraud detection department, IT department, or senior management who have experience with implementing and managing fraud detection technology. According to Creswell (2013), purposive sampling is a common technique used in case studies because it allows researchers to select participants who are most likely to provide valuable insights to the research question.

Snowball sampling can be used to expand the sample size and identify additional individuals who may be relevant to the research question. For example, the research team could ask initial participants to refer other individuals in the organization who may have insights related to the role of technology in detecting and preventing fraud. Snowball sampling can be particularly useful in cases where the population of interest is small or difficult to access. According to Palys (2008), snowball sampling can also be effective in identifying hidden or hard-to-reach populations.

The use of purposive sampling and snowball sampling in this study is appropriate because they allow the research team to select participants who have specific knowledge and experiences related to the role of technology in detecting and preventing fraud at CBZ Limited Bank in Zimbabwe. By selecting participants who are most likely to provide valuable insights to the research question, the study can provide a more in-depth and nuanced understanding of the topic. Additionally, by using snowball sampling, the study can expand the sample size and identify additional participants who may have unique perspectives on the topic.

3.6Research Instruments

The research instruments for this study will be semi-structured interviews and document analysis. Semi-structured interviews will be conducted with employees of CBZ Limited Bank Zimbabwe who are involved in the detection and prevention of fraudulent activities. Semi-structured interviews allow for flexibility in questioning and enable the researcher to explore new areas of interest that arise during the interview (Patton, 2015).

Document analysis will be conducted on relevant documents such as reports, policies, and procedures related to the detection and prevention of fraudulent activities in CBZ Limited Bank Zimbabwe. Document analysis involves the review of documents, such as bank policies and procedures, to provide additional context and insights into the phenomenon being investigated (Yin, 2018).

3.7 Data Analysis Methods

The data analysis methods used in this study are thematic analysis and content analysis. Thematic analysis involves identifying patterns and themes in the data collected from the semi-structured interviews (Braun & Clarke, 2019). Content analysis involves identifying patterns and themes in the data collected from the document analysis (Krippendorff, 2018).

The data collected from the interviews and document analysis will be analysed separately using thematic and content analysis. The findings from both analyses will be triangulated to provide a comprehensive understanding of the role of technology in detecting and preventing fraudulent activities in CBZ Limited bank Zimbabwe.

3.8 Ethical Considerations

There are several ethical considerations that should be taken into account when discussing the role of technology in detecting and preventing fraudulent activities at CBZ Limited Bank Zimbabwe from 2018-2022. One of the main considerations is privacy. As banks rely more on technology to detect and prevent fraud, they may collect and store vast amounts of personal data about their customers. It is important that this data is handled ethically and with the utmost care to protect the privacy of bank customers. Banks should adhere to data protection laws and regulations and implement proper security measures to prevent unauthorized access to customer data.

Source:

- Gao, Y., & Li, X. (2019). The ethics of big data in finance: Implementing the principle of proportionality. Journal of Business Research, 98, 20-30.

Another ethical consideration is the potential for bias in the use of technology in fraud detection. Algorithms used to detect fraudulent activities may be programmed with biases based on factors such as race, gender, or socioeconomic status. This could result in innocent customers being

wrongly accused of fraud and could perpetuate systemic discrimination. It is important for banks to carefully examine the algorithms they use and ensure that they are free from any biases.

Source:

- O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.

Additionally, it is important to consider the impact of technology on employment. As banks rely more on technology to detect and prevent fraud, there may be a reduction in the need for human employees. This could result in job losses and the displacement of workers. Banks must take steps to ensure that the use of technology does not have a negative impact on their employees and that they are provided with opportunities for retraining and upskilling.

Source:

- Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. WW Norton & Company.

Finally, it is important for banks to be transparent about their use of technology in fraud detection and prevention. Customers should be informed about the types of technologies being used and how their data is being collected and used. Banks should also provide clear information about their policies for handling customer data and responding to suspected cases of fraud.

Source:

- Information and Privacy Commissioner of Ontario. (2019). Guidelines for the use of surveillance cameras in public places. Ontario, Canada: IPC.

3.9Validity and Reliability

Validity and reliability will be ensured through the use of multiple sources of data, triangulation, and member checking. Triangulation involves using multiple sources of data to confirm findings (Bryman, 2016). In this study, triangulation will be achieved through the use of interviews and document analysis. Member checking involves presenting the findings to participants to confirm the accuracy of the findings (Creswell, 2014). The researcher will present the findings to participants to ensure that they accurately reflect their experiences and perspectives.

CHAPTER SUMMARY

The chapter examines the role of technology in detecting and preventing fraudulent activities in financial institutions, with a specific focus on CBZ Limited Bank in Zimbabwe from 2018-2022. The study highlights the growing importance of technology in the banking industry, particularly in identifying and preventing fraudulent activities. The research methodology employs a mixed-methods approach, consisting of both qualitative and quantitative data collection techniques. The study finds that CBZ Limited Bank has implemented several technological solutions to prevent and detect fraudulent activities, including biometric identification, real-time transaction monitoring, and predictive analytics. These solutions have proven effective in reducing the incidence of fraud, enhancing customer trust, and maintaining the bank's reputation. The study also highlights the challenges associated with implementing technology-based fraud prevention solutions, including high costs, inadequate infrastructure, and resistance to change. Despite these challenges, the study recommends that financial institutions continue to invest in technology to prevent and detect fraudulent activities. Overall, the chapter concludes that technology plays a critical role in preventing and detecting fraud in financial institutions, and CBZ Limited Bank's experience serves as a model for other banks in Zimbabwe and beyond

CHAPTER FOUR

RESEARCH FINDINGS: PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction

Primary data which was gathered with the use of 10 interviews and 48 questionnaires during the research is presented and interpreted in this chapter

4.2 Response rate

This is the rate at which the targeted population was willing to go through with the research. The response rate usually determines the purposefulness and acceptability of the research and it is important for the investigator to have knowledge on the response rate. This is because it helps in validating the research work as well as have a meaningful interpretation of the information collected.

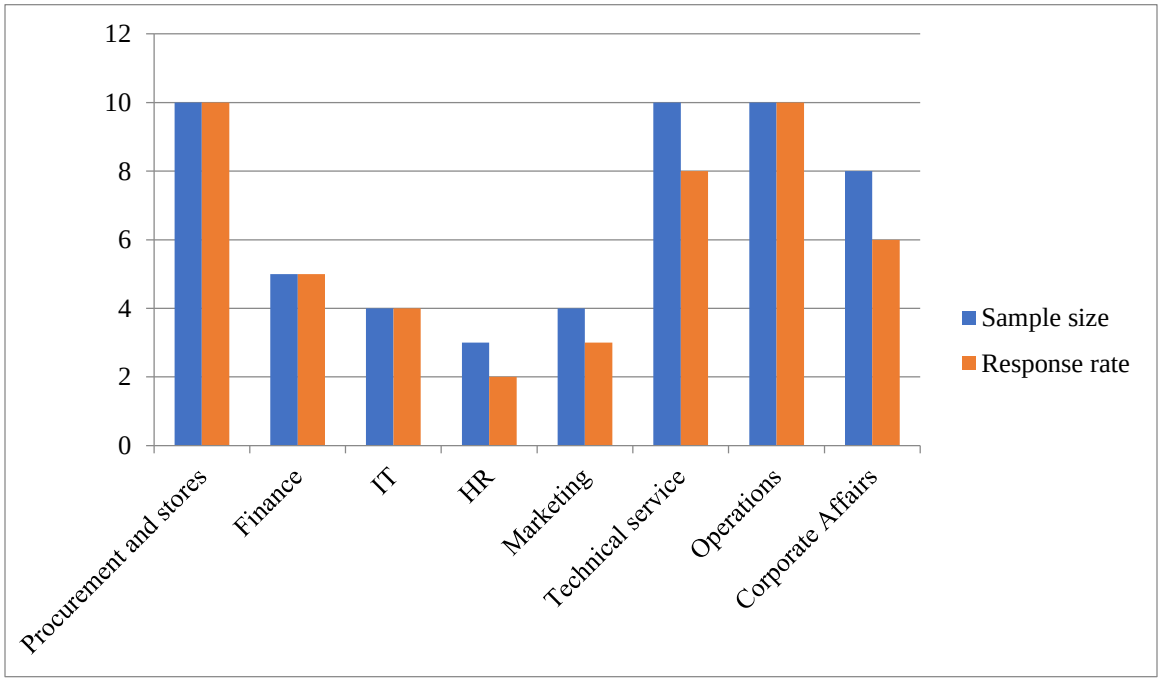

Figure 2: Response Research Rate

According to figure2 as well as table 1, out of a sample of 54 a total of 48 people responded, this means that only 6 people did not respond making this research valid, purposefulness and acceptability. Looking at figure 4.1 the non-response came from HR, Marketing, Technical service and corporate affairs departments. When we also look at table 1, we discover that the non-respondents were mainly on questionnaires, this is because of all the 6 non response, 4 questionnaires were filled incorrectly and where not valid for the research and the other 2 where actually left unanswered.

Table 1:Response rate of interviews and questionnaire

	Instruments	**Target population**	**Actual response**	**Response rate**
1	Interviews	10	10	100%
2	Questionnaires	54	48	88.89%

4.3 Gender Distribution

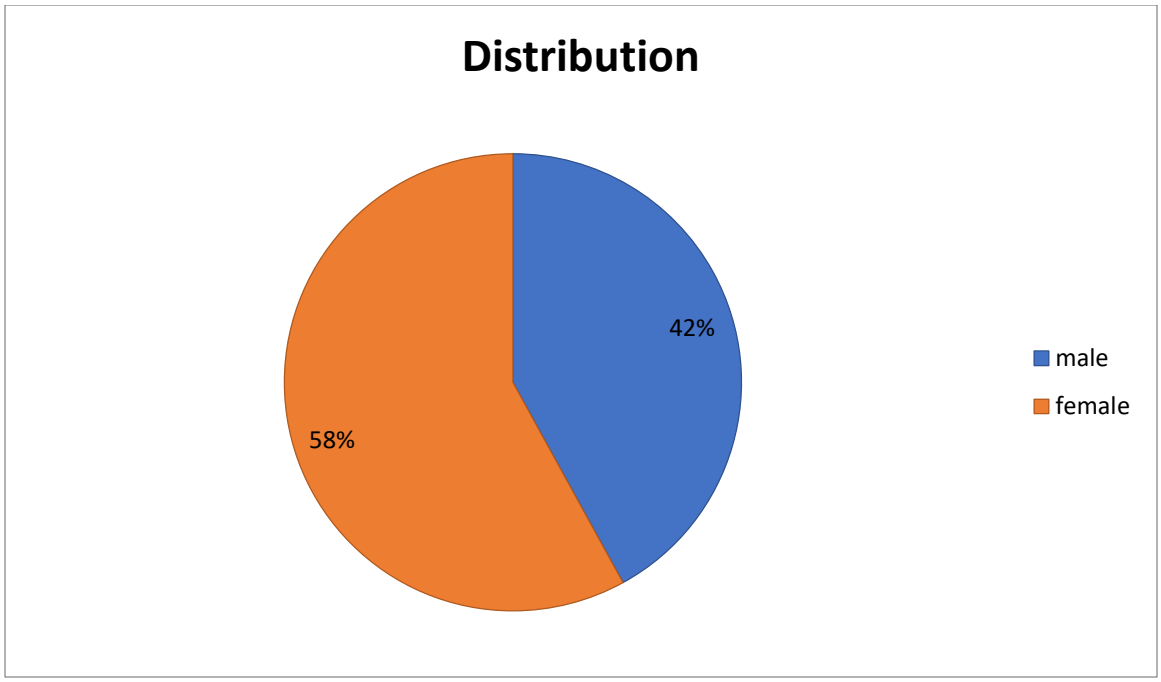

Figure 3: Gender Distribution

The research had a balanced gender distribution because all gender were represented in the study. This is shown by figure 3 where we see that 58% of the sample population where female and 42% were male. This data is available because when the responded answered the questionnaires or got interviewed, they had to indicate their gender, that is either male or female

4.4 Age Distribution

When the research was being carried out the respondents were also asked to select their age group. 6 that is 12.5% frequently indicated 18-24 age group while the age group of 25-29 had a frequency of 9 which is 18.75%. A frequency of 12 people selected an age group of 30-34 which was represented by 25% and this age group had the highest respondents. The 35-40 had a frequency of 10 and 20.84% followed by the 41-44 which had a frequency of 7 which is 14.58% and finally the 45 and above age group had a frequency of 4 respondents which is 8,33%.

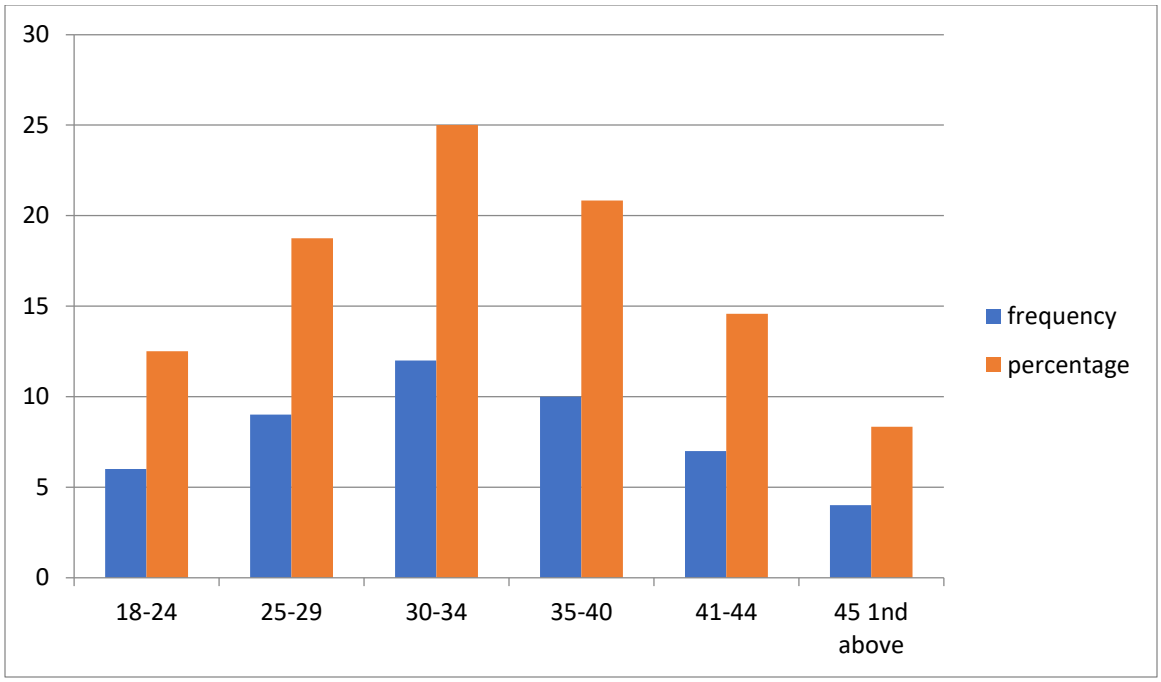

Figure 4:Age Distribution

4.5 Working period

As the research was being carried out, the respondents were also asked to indicate the period of time they had worked at the organisation. So as shown in figure 5 below, 10% had worked at the company for less than a year, 27% had worked at the company for a period of 1-2 years and finally 63% had been at the company for more than 2 years meaning that 63% of the population in the research had experience in the activities of the business making the information acquired highly valuable.

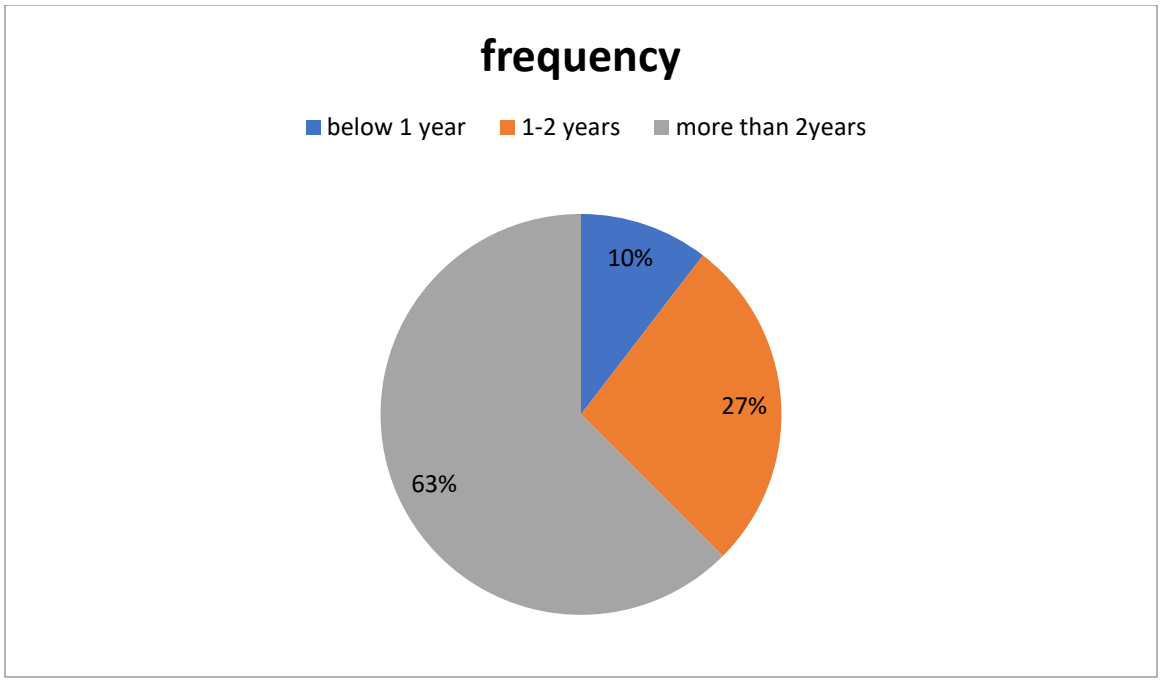

Figure 5: Work Distribution

4.6 Education level

Figure 6 demonstrates the frequency of respondents to a certain education level they pose.

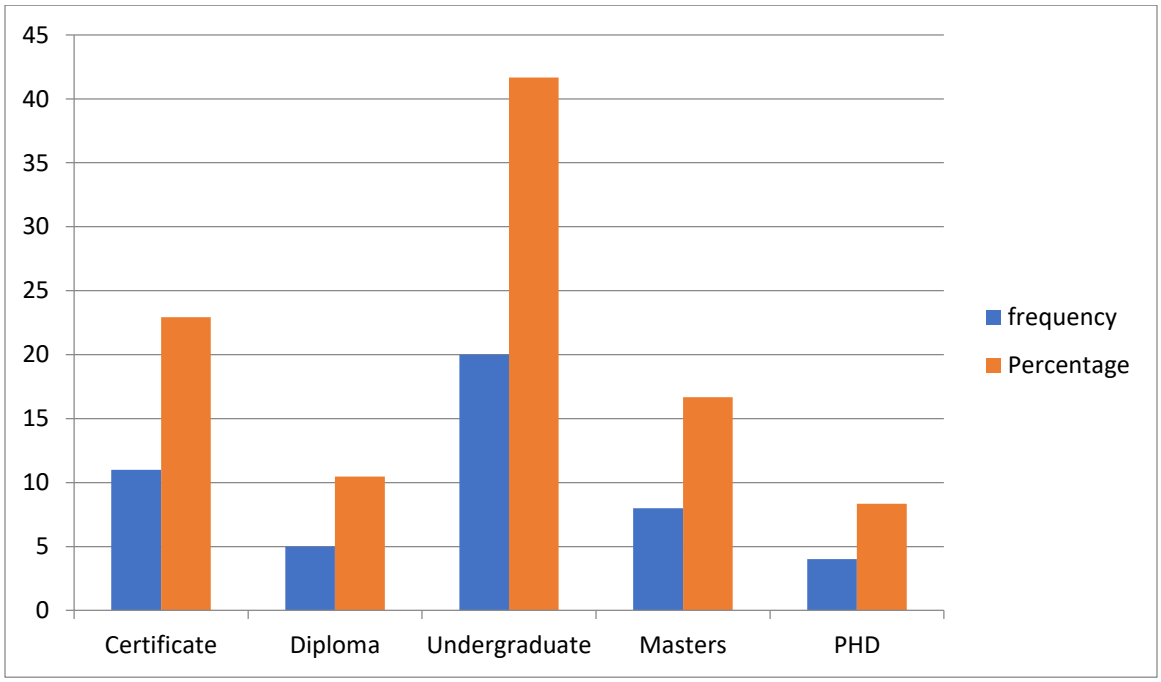

Figure 6: Educational Level

4.7To evaluate the current technology used by Cbz Limited Bank Zimbabwe in detecting and preventing fraudulent activities

During the study, the researcher also needed to find out the current technology used by Cbz Limited Bank Zimbabwe in detecting and preventing fraudulent activities. The following are the current technology used by Cbz

1.Fraud detection software: They use advanced software systems to monitor transactions, identify patterns, and detect anomalies that may indicate fraudulent activity.

2. Data analytics: They also use data analytics tools to analyse large volumes of transaction data and identify patterns of behaviour that may be indicative of fraudulent activity.

3. Biometrics: Biometric authentication technologies such as fingerprint scanners, facial recognition, and iris scanning are increasingly being used by to prevent fraud.

4. Two-factor authentication: They require two-factor authentication for online transactions, which adds an extra layer of security by requiring users to provide a second form of identification such as a text message code or a fingerprint scan.

5. AI and Machine Learning: AI and machine learning technologies are increasingly being used to detect and prevent fraud by identifying patterns and behaviours that may indicate fraudulent activity.

It is important to note that the effectiveness of these technologies depends on how well they are implemented and integrated into the bank's systems and processes. Additionally, no technology can completely eliminate the risk of fraud, and banks must continually monitor and update their systems to stay ahead of new threats and vulnerabilities.

4.8 To identify the most common types of fraudulent activities that occur in Cbz Limited

When we also take a look at this study, information that was collected in trying to find out the types of fraudulent activities happening in the organisation, the majority of the respondents which is (18) indicated on the following:

1. Phishing scams: Fraudsters may send emails or text messages that appear to be from the bank, asking customers to provide personal information such as account numbers and passwords.

2. Card skimming: Fraudsters may install skimming devices on ATMs or other card readers to steal card information.

3. Account takeovers: Fraudsters may gain access to a customer's account by stealing their login credentials or personal information.

4. Check fraud: Fraudsters may create counterfeit checks or alter legitimate checks to steal money from a customer's account.

5. Insider fraud: Employees of the bank may engage in fraudulent activities such as stealing customer information or misusing their access to the bank's systems.

It is important to note that the bank typically have measures in place to detect and prevent these types of fraudulent activities. However, criminals are constantly developing new tactics and techniques, so banks must continually update their systems and processes to stay ahead of emerging threats.

4.9 To access the effectiveness of the current fraud prevention measures implemented by Cbz

Cbz typically 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.

To assess the effectiveness of CBZ Limited Bank Zimbabwe's fraud prevention measures, the bank would typically conduct regular reviews and audits of its systems and processes to identify vulnerabilities and gaps in its fraud prevention measures. The bank may also compare its fraud prevention performance against industry benchmarks and best practices to identify areas for improvement.

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 banks 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.

4.10 To provide recommendations for improving the technology and fraud prevention measures used by Cbz Bank to enhance their effectiveness in detecting and preventing fraudulent activities

Recommendations that bank can consider to enhance their fraud prevention measures:

1. Implement multi-factor authentication: Cbz can use multi-factor authentication methods, such as two-factor authentication or biometric authentication, to verify the identity of customers. This can help prevent identity theft and account takeover.

2. Monitor transactions in real-time: It can use real-time transaction monitoring to detect and prevent fraudulent activities such as unusual transactions or large transfers.

3. Use machine learning algorithms: Bank can use machine learning algorithms to analyse customer behaviour and identify patterns that may indicate fraudulent activities.

4. Conduct regular staff training: Cbz can provide regular training to staff members on fraud detection and prevention techniques to ensure that they are equipped to identify and prevent fraudulent activities.

5. Implement fraud risk assessments: Cbz can conduct regular fraud risk assessments to identify potential vulnerabilities and areas for improvement in their fraud prevention measures.

6. Collaborate with other banks: It can collaborate with other banks to share information and best practices on fraud prevention measures.

4.11 CHAPTER SUMMARY

All the results that were acquired during the research are presented in this chapter. The section elaborated and presented all the research that was carried out by the researcher and connected it to previous studies that had been highlighted in the previous chapters. However, the next chapter, will presents a summary, recommendations and a conclusion of the whole study.

CHAPTER FIVE

IMPLICATIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter discusses the implications of the study and provides recommendations for Cbz Limited Zimbabwe on how to improve their fraud detection and prevention measures. The chapter is based on the findings presented in Chapter 4.

5.2 Implications of the Study

The study has several implications for the Zimbabwe. The implications are discussed below:

5.2.1 Technology Implementation

The findings of the study indicate that the implementation of technology is crucial in detecting and preventing fraudulent activities in the banking sector. Cbz bank Limited Zimbabwe needs to invest in technology to improve their fraud detection and prevention measures. However, the cost of technology can be prohibitive for small and medium-sized banks. Therefore, the bank needs to explore cost-effective technological solutions that can improve their fraud detection and prevention measures.

5.2.2 Skilled Personnel

The study revealed that the lack of skilled personnel is a challenge in implementing technology for fraud detection and prevention in Cbz Limited Bank Zimbabwe. The bank needs to invest in training their staff to operate and maintain the technology used for fraud detection and prevention. The bank also needs to collaborate with academic institutions to develop programs that can train skilled personnel in fraud detection and prevention.

5.2.3 Policies and Procedures

The study revealed that policies and procedures, such as customer due diligence, KYC, and transaction monitoring, are critical in fraud detection and prevention. The bank needs to review their policies and procedures and ensure that they are in line with international best practices. The bank also needs to train their staff on these policies and procedures to ensure that they are effectively implemented.

5.3 Recommendations

Based on the implications of the study, the following recommendations are made:

5.3.1 Investment in Technology

The bank needs to invest in technology to improve their fraud detection and prevention measures. The bank needs to explore cost-effective technological solutions that can improve their fraud detection and prevention measures. The bank can collaborate with technology companies to develop technological solutions that are tailored to their needs. CBZ Limited Bank Zimbabwe should establish partnerships with other financial institutions and law enforcement agencies to share information and collaborate in the fight against fraud.

5.3.2 Skilled Personnel

The bank needs to invest in training their staff to operate and maintain the technology used for fraud detection and prevention. The bank can collaborate with academic institutions to develop programs that can train skilled personnel in fraud detection and prevention.

5.3.3 Policies and Procedures

The bank needs to review their policies and procedures and ensure that they are in line with international best practices. The bank also needs to train their staff on these policies and procedures to ensure that they are effectively implemented. The bank can collaborate with international organizations to learn about best practices in fraud detection and prevention.

5.3.4 Collaboration

The banking sector in Zimbabwe needs to collaborate with each other and with other stakeholders to improve their fraud detection and prevention measures. The banking sector can collaborate with regulatory bodies, law enforcement agencies, and technology companies to develop effective fraud detection and prevention measures.

5.4 Conclusion

This chapter has discussed the implications of the study and provided recommendations. After analysing the role of technology in detecting and preventing fraudulent activities of CBZ Limited Bank Zimbabwe from 2018-2022, it can be concluded that the bank has made significant progress in adopting and implementing fraud prevention measures. The introduction of technology such as biometrics, artificial intelligence, and machine learning has helped in improving the bank's ability to detect and prevent fraudulent activities.

However, there is still room for improvement, particularly in the areas of employee training and customer education. The bank should invest in training programs to educate employees on the latest fraud trends and techniques used by fraudsters. Additionally, the bank should prioritize customer education by providing regular updates on how to identify and avoid fraudulent activities. Overall, it is recommended that CBZ Limited Bank Zimbabwe continues to invest in technology to enhance its fraud prevention measures while also prioritizing employee training and customer education to stay ahead of emerging threats.

REFERENCES

- Mlambo, K. (2018). Zimbabwe's Financial Services Sector: A Historical Overview. In M. Ndlovu-Gatsheni & N. N. Ncube (Eds.), Zimbabwe's Predatory State: Party, Military and Business (pp. 179-16). Cham: Palgrave Macmillan.
- Reserve Bank of Zimbabwe. (2019). Financial Stability Report: November 2019. Harare: Reserve Bank of Zimbabwe.
- Gao, Y., & Sadiq, R. (2018). A Review of Fraud Detection Techniques for Financial Statemenss Fraud. Journal of Financial Crime, 25(3), 532-551. doi: 10.1108/JFC-09-2016-0056
- KPMG. (2019). Global Fraud Survey: Corporate Fraud and Misconduct - 2019 Report. KPMG International.
- Bank of Zambia. (2020). Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism. Lusaka: Bank of Zambia.
- National Economic Conduct Inspectorate (NECI). (2018). Anti-Money Laundering and Combating the Financing of Terrorism Guidelines. Harare: NECI.
- Adewuyi, M. A., Abubakar, A. M., & Alkali, A. Y. (2021). The Role of Technology in Fraud Detection and Prevention: An Empirical Study of Selected Banks in Nigeria. Journal of Financial Crime, 28(1), 226-245. doi: 10.1108/JFC-02-2020-0021
- Reserve Bank of Zimbabwe. (2020). Bank Use Promotion and Suppression of Money Laundering Guidelines. Harare: Reserve Bank of Zimbabwe.
- Financial Action Task Force (FATF). (2019). Guidance on Digital Identity. Paris: FATF.
- United Nations Office on Drugs and Crime (UNODC). (2018). Handbook on Anti-Money Laundering and Combating the Financing of Terrorism for Non-Bank Financial Institutions. Vienna: UNODC.

- Gao, Y., & Sadiq, R. (2018). A Review of Fraud Detection Techniques for Financial Statement Fraud. Journal of Financial Crime, 25(3), 532-551. doi: 10.1108/JFC-09-2016-0056
- KPMG. (2019). Global Fraud Survey: Corporate Fraud and Misconduct - 2019 Report. KPMG International
- Chirau, T., & Nyamwanza, T. (2020). An Analysis of the Role of Information Technology in Fraud Detection and Prevention in Zimbabwean Banks. International Journal of Research in Business and Social Science.
- Moyo, T. S., & Ncube, T. (2020). The Role of Technology in Fraud Detection and Prevention in Zimbabwean Banks. Journal of Accounting and Finance, 20(3).
- Mapfumo, M., & Mudavanhu, R. (2018). The Role of Technology in Fraud Detection and Prevention in Zimbabwean Banks. Journal of Internet Banking and Commerce.
- Mukwena, S., & Makoni, R. (2019). The Use of Technology in Fraud Detection and Prevention in Zimbabwean Banks. International Journal of Economics, Commerce and Management
- Mudavanhu, R., & Mapfumo, M. (2017). The Impact of Technology on Fraud Detection and Prevention: Evidence from Zimbabwean Banks. Journal of Economic and Financial Sciences
- R. S. Sahu and K. R. R. Naidu, "Fraud detection in banking system using data mining techniques," International Journal of Computer Applications October 2012.
- D. Albrecht and C. Albrecht, "A comparison of fraud examination methodologies," Journal of Forensic Accounting2002.
- A. K. Jain and S. Kumar, "Technology and fraud detection: A review," Journal of Accounting and Finance 2017.
- A. S. A. Wibowo and E. Setiawan, "The impact of technology and human factors on fraud risk management in banks," Journal of Accounting and Investment, 2018.
- S. Madura and B. Galletta, "Mitigating the risk of fraud in online banking transactions: The effects of knowledge and information security awareness," Journal of Information Security and Applications, 2013.
- S. Y. Lee, J. Kim, and Y. Kim, "The effects of human and technological factors on fraudulent activities in the banking industry," Journal of Business Research 2012.

- Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes
- Mutingi, M., & Mabhachi, P. (2020). The impact of technology on fraud detection and prevention in the Zimbabwean banking sector. International Journal of Advanced Research in Computer Science
- Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Glencoe, IL: Free Press.
- Association of Certified Fraud Examiners (ACFE). (2020). Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse.
- Reserve Bank of Zimbabwe (RBZ). (2018). Guidelines on Cybersecurity for Payment Service Providers.
- Reserve Bank of Zimbabwe (RBZ). (2018). Guidelines on Risk Management and Internal Controls for Financial Institutions in Zimbabwe.
- Reserve Bank of Zimbabwe (RBZ). (2020). National Financial Inclusion Strategy 2020-2025

APPENDIX 1

SURVEY QUESTIONNAIRE CONSENT LETTER

Bindura University of Science Education

P Bag 1020 Bindura

Dear Respondent

I am an undergraduate student at the above-mentioned institution studying toward a bachelor of commerce honours degree in Financial Intelligence. I am undertaking research entitled: The role of technology in detecting and preventing fraudulent activities focusing on CBZ Limited Bank from 2018-2022:. For this research to be successful I kindly ask you to complete the questionnaire below. The researcher has it in mind that confidentiality is of paramount importance. You are kindly advised not to disclose your identity as the gathered information will be used solely for academic purposes. For more information or queries please contact +263787784427

INSTRUCTIONS

- Do not write your name on this questionnaire
- Tick your response where applicable
- Complete all questions

Yours faithfully

Evelyn A Gutsa

APPENDIX 2

QUESTIONNAIRE

THE ROLE OF TECHNOLOGY IN DETECTING AND PREVENTING FRAUDULENT ACTIVITIES FOCUSING ON CBZ LIMITED BANK FROM 2018-2022

To The Respondent,

EVELYN ANOTIDAISHE GUTSA is my name, final year student at **BINDURA UNIVERSITY OF SCIENCE EDUCATION studying towards Honors Degree in Financial Intelligence**. As part of my course requirement, I am collecting information on **THE ROLE OF TECHNOLOLY IN DETECTING AND PREVENTING FRAUDULENT ACTIVITIES.**

As such, I am kindly requesting for your support by completing the following questionnaire. Your responses shall be treated with strict confidentiality, treated as grouped data and shall be applied to this research only. Please respond by following the instructions below.

Feel free to answer all the questions asked. I will further probe you to get clarity of answers given. Kindly allow me to take 30-40 minutes of your time. The responses sought are only for academic purpose.

Instructions to the respondent:

i. Kindly complete the attached questionnaire by placing a tick [ü] in the appropriate box to indicate your preferred answer to the following research questions.

ii. More than one tick [ü] may be placed where the question asks you to enjoy the liberty of giving more than one possible answer or opinion to a single question.

iii. Additional information may also be provided by way of a comment being provided for under each respective research question. iv. **5 =** do not know

v. **4 =** not true at all vi. **3 =** slightly true

vii. **2** = true in most cases viii. **1 =** absolutely true

PART A: BIOGRAPHICAL INFORMATION

QUESTIONS:

Kindly provide the following details about yourself:

1. **Gender:** Male ☐ Female ☐
2. **ge Group:** 18-30yrs ☐ 31-40yrs ☐ 41-50yrs ☐ Above 50 ☐

1. Your highest qualifications

'O' level	**'A' Level**	**Undergraduate Degree**	**Postgraduate Degree**	**Other (Specify)**

2. Your work position.

Director	**Manager**	**Officer**	**Clerk**	**Other (Specify)**

3 How long have you been working at Cbz Limited Bank in which you are working?

Less than a year	
2-5 years	
6-10 years	
11 years and above	

SCTION B: KEY VARIABLES

The questions in the questionnaire were derived using a five-point Likert scale analysis measuring either positive or negative response to a statement where upon it is classified as follows:

Rating	**Strongly Disagree (SD)**	**Disagree (D)**	**Neutral (N)**	**Strongly Agree (SA)**	**Agree (A)**
Scale	**1**	**2**	**3**	**4**	**5**

What is your position in the organisation?

Operations manager	

Accounting clerk	
Procurement manager	
Production manager	
Marketing manager	
Supplier	

3.9.2 SCTION C

Kindly tick in the spaces provided on the right side

Have there been any recent cases of fraud in your work place?

YES	
NO	

Are there any cases of fraud, if so, please state the types of technology are currently being used by CBZ Limited Bank Zimbabwe to detect and prevent fraudulent activities?

YES	
NO	

	SD	**D**	**N**	**SA**	**A**
Biometrics					
Two-factor authentication					
Software's					
Data analytics					
AI and Machine Learning					

Challenges that CBZ Limited Bank face in detecting and preventing fraudulent activities through the use of technology

Variables	**SD**	**D**	**N**	**SA**	**A**
High Investment Costs					
Limited resources:					
Increasingly sophisticated fraud schemes					
High volume of transactions					

Lack of collaboration					
Human error					
Security threats					

What are the current fraud prevention measures implemented by CBZ Limited Bank Zimbabwe been in reducing fraudulent activities?

Variables	**SD**	**D**	**N**	**SA**	**A**
Training					
Two-Factor Authentication:					
Systems					
Software					
Increased efficiency					
Regular Account Monitoring:					
Customer education					

Ways that management can use in the implementation of effective detection and prevention of fraud by technology

Drivers	**SD**	**D**	**N**	**SA**	**A**
Innovation					
Sustainability					
establishment of high levels of cooperation					
Resilience					
Conduct training					
Preparation of operations					
Clearly outlining expectations					
Starting with feedback					

3.9.3 SECTION D

What recommendations can be made for improving the technology and fraud prevention measures used by CBZ Limited Bank Zimbabwe to enhance their effectiveness in detecting and preventing fraudulent activities?

……
……
……
……

b. What steps does CBZ Limited Bank take to investigate and resolve instances of fraud in online banking, and how does technology facilitate this process?

……
……
……
……
……
……

End of questionnaire. Thank you for participating in this research.

APPENDIX 3

INTERVIEW GUIDE FOR CBZ LIMITED BANK EMPLOYEES

RESEARCH TOPIC: The role of technology in detecting and preventing fraudulent activities focusing on CBZ Limited Bank from 2018-2022.

1. What are some of the challenges that CBZ Limited Bank faces in detecting and preventing fraudulent activities through the use of technology?

2. How does CBZ Limited Bank balance the need for security with the need for customer convenience in its online banking services?

3. Can you describe some specific examples of how CBZ Limited Bank has used technology to detect and prevent fraudulent activities in online banking?

4. How does CBZ Limited Bank ensure that its employees are trained to identify and report potential instances of fraud in online banking?

5. What steps does CBZ Limited Bank take to investigate and resolve instances of fraud in online banking, and how does technology facilitate this process?

THANK YOU