

BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES



DISSERTATION RESEARCH PROJECT

**THE ROLE OF TECHNOLOGY IN FINANCIAL CRIME PREVENTION: A CASE
STUDY OF ZIMBABWE'S BANKING SECTOR**

BY

GENNAH GOMBE B222358B

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

2026

RELEASE FORM

Registration number : B222358B

Dissertation title: The Role of Technology in Financial Crime Prevention: A Case Study of Zimbabwe's Banking Sector.

Degree title: Bachelor of Commerce Honours Degree in Financial Intelligence

Year granted: 2026

Permission is granted to the Bindura University Library to produce one copy of the thesis to be used for private, scientific or academic purposes, and for lending and selling of such copies. The other publishing rights are reserved by the author. The thesis and parts thereof are not to be printed or published in any manner whatsoever, without written consent from the author.

Signed: -----

Date: -----

APPROVAL FORM

The undersigned has read and accepted the project and submitted for evaluation and approval of Bindura University of Gennah Gombe. It bears the title "The role of Technology in Financial Crime prevention: A case study of Zimbabwe's banking sector" for partial fulfillment of the requirements for Bachelor of Commerce Honours Degree in Financial Intelligence.



Student.....Date...17.08.2026.....



Supervisor: ...E Maravanyika...Date...31 July 2026.....



Chairperson of Department..... Date.....18/08/26.....

DEDICATION

I would like to dedicate this dissertation to my family. You made it possible for me to complete this, and without your love, sacrifices, and faith in me this would not have been completed. To all of the people that helped me dream big and still supported me when I did: this is for you.

ACKNOWLEDGEMENTS

I would like to express my extended gratitude to my supervisor, Mr. Maravanyika, for his immense knowledge and experience and the useful advice given. My thanks to the Faculty of Commerce, Bindura University of Science Education, the respondents from CBZ Holdings and FBC Holdings, as well as my lecturers who played a part in my academic journey. I am so grateful to my family and friends who have stood by me in this endeavor.

ABSTRACT

This study sought to investigate the extent to which technology is used in preventing financial crime at CBZ holdings and FBC holdings. The study was triggered by the occurrence of financial crimes even with increased expenditure on the development and adoption of technology systems. The study design was a mixed methods case study. Fifty questionnaires were distributed to bank employees and ten semi-structured face-to-face interviews were conducted with bank employees. Questionnaires were analysed using descriptive statistics and interview data through thematic analysis. The results show that rule-based systems were predominantly used as opposed to artificial intelligence and machine learning which were the least utilized. Implementation challenges included false positives, high capital expenditure, lack of synergy between the banking sector and lack of effective staff training. Conclusion is that it is not only technology that will curb the occurrence of financial crime in banking institutions but there must also be corresponding human capacity and appropriate institutional structures. The researcher recommends the increased investment of advanced technology in banking and staff training as well as improved coordination with FIUZ.

Table of Contents

RELEASE FORM.....	ii
APPROVAL FORM	iii
DEDICATION	iv
ACKNOWLEDGEMENTS	v
ABSTRACT	vi
TABLE OF FIGURES	xi
LIST OF TABLES	xii
LIST OF ABBREVIATIONS	xiii
CHAPTER ONE	1
INTRODUCTION	1
1.0 Introduction	1
1.1 Background of the Study	1
1.2 Problem Statement	6
1.3 Purpose of the Study	7
1.4 Objectives of the Study	7
1.5 Research Questions	7
1.6 Significance of the Study	7
1.6.1 To the researcher	8
1.6.2 Policy Makers (RBZ and FIUZ)	8
1.6.3 Banking Institutions	8
1.6.4 Academia and Future Researchers	8
1.7 Assumptions of the Study	8
1.8 Delimitations of the Study	9
1.9 Limitations of the Study	9
1.10 Definition of Terms	10

1.10 Dissertation outline	11
1.11 Chapter Summary.....	11
CHAPTER TWO	13
LITERATURE REVIEW	13
2.0 Introduction	13
2.1 Conceptual Framework	13
2.1.1 Conceptualising Financial Crime.....	13
2.1.2 Technological Solutions for Financial Crime Prevention	14
2.1.3 Classification of Technologies	15
2.3 Theoretical Framework	16
2.3.1 Diffusion of Innovations Theory.....	17
2.3.2 Technology Acceptance Model.....	18
2.3.3 Integration of Theories.....	18
2.4 Empirical Evidence	19
2.4.1 Global Studies.....	19
2.4.2 African Studies.....	20
2.4.3 Zimbabwean Studies.....	20
2.5 Research Gap.....	21
2.6 Chapter Summary.....	23
CHAPTER THREE	24
METHODOLOGY	24
3.0 Introduction	24
3.1 Research Philosophy	24
3.2 Research Approach	25
3.3 Research Design.....	25
3.4 Study Population	26
3.5 Sample size and Sampling Techniques	27

3.6 Research Instruments	29
3.6.1 Questionnaire	29
3.6.2 Semi-structured Interview Guide	30
3.7 Pilot Testing	30
3.8 Validity and Reliability	31
3.9 Data Collection Procedure	32
3.10 Data Analysis Techniques	32
3.11 Ethical Considerations.....	33
3.12 Limitations of the Study	33
3.12 Chapter Summary.....	34
CHAPTER FOUR.....	35
DATA ANALYSIS, INTERPRETATION AND PRESENTATIONS	35
4.1 Introduction	35
4.2 Response Rate	35
4.3 Demographic Profile of Respondents	36
4.4 Research Findings and Discussion.....	39
4.5 Technologies Used for Financial Crime Detection	41
4.6 Effectiveness of Current Technologies	43
4.7 Challenges Affecting Technology Use	44
4.8 Interview Findings.....	46
4.9 User Training and Acceptance	48
4.10 Chapter Summary.....	49
CHAPTER FIVE	51
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS.....	51
5.1 Introduction	51
5.2 Findings.....	51

5.3 Conclusions	52
Overall Conclusion:.....	53
5.4 Contribution to Knowledge	53
5.5 Limitations of the Study	54
5.6 Recommendations	55
5.6.1 Recommendations for Practice	55
5.6.2 Recommendations for Future Research	55
REFERENCES	57
APPENDIX 1.....	61
APPENDIX 2.....	62
QUESTIONNAIRE	62
APPENDIX 3.....	67
SEMI-STRUCTURED INTERVIEW GUIDE	67
APPENDIX 4: TURNITIN REPORT	68

TABLE OF FIGURES

Figure 1: Conceptual Framework for The Role of Financial Crime Prevention in Zimbabwe's Banking Sector.....	16
Figure 2: Gender distribution.....	38
Figure 3: Age distribution.....	39
Figure 4: Technology adoption.....	42
Figure 5: Effectiveness mean score	44
Figure 6: Challenges ranking.....	46
Figure 7: User acceptance statement:	49

LIST OF TABLES

Table 1: Classification of Financial Crime Prevention Technologies	15
Table 2: Sample Constituency.....	27
Table 3: Questionnaire Response Rate	35
Table 4: Interview Completion Rate.....	36
Table 5: Demographic Characteristics of Respondents	36
Table 6: Technology Adoption by Bank.....	41
Table 7: Perceived Effectiveness (Likert Scale: 1–5).....	42
Table 8: Operational Challenges (Likert Scale: 1–5)	44
Table 9: User Training and Acceptance.....	48

LIST OF ABBREVIATIONS

Abbreviation	Full Form
AI	Artificial Intelligence
AML	Anti-Money Laundering
CBZ	CBZ Holdings
CDD	Customer Due Diligence
CTF	Counter-Terrorist Financing
FATF	Financial Action Task Force
FBC	FBC Holdings
FIU	Financial Intelligence Unit
FIUZ	Financial Intelligence Unit of Zimbabwe
IT	Information Technology
ML	Machine Learning
RBZ	Reserve Bank of Zimbabwe
RegTech	Regulatory Technology
RTGS	Real-Time Gross Settlement
STR	Suspicious Transaction Report
TAM	Technology Acceptance Model
UNODC	United Nations Office on Drugs and Crime
ZRP	Zimbabwe Republic Police
ZWL	Zimbabwean Dollar (Zimbabwe Dollar)

CHAPTER ONE

INTRODUCTION

1.0 Introduction

Digital financial services are rapidly growing, and financial crime is getting more sophisticated in the financial sector. As a result of the shift of the banking operations to the online space through the elimination of physical branches and their replacement with websites, money laundering, fraud, and terrorist financing techniques have evolved as well. The current paper examines the possible application of the technology in combating known financial crimes such as terrorist financing fraud, and money laundering in the banking sector of Zimbabwe.

In the last ten years, there has been an unprecedented revolution in the financial sector of Zimbabwe caused by cash liquidity problems and the development of mobile banking (Reserve Bank of Zimbabwe, 2020). Nevertheless, this process has revealed certain structural weaknesses of the country. It is important to mention that international organisations and the FIUZ emphasise the importance of the use of modern technologies to combat new financial crimes. This chapter introduces the background, the problem statements, and objectives of the study.

1.1 Background of the Study

The Global Context

Financial crime has evolved significantly with the rapid digitalisation of global financial systems. It is true that crimes of fraud, such as embezzlement and forgery, are still around. However, as technology has developed, so has crime, in ways such as, cyber enabled fraud, identity theft and the advanced planning of laundering schemes. This increase in the ways crimes can be committed, combined with the spread of technology throughout the world means that illicit financial flows reach their target quicker and further afield, as reported by the UNODC (2022), where the introduction of digital financial platforms has increased both the speed and reach of these illicit flows, hence increasing the difficulty to detect and prevent them.

The number of financial losses suffered by financial institutions around the world are enormous. For example, Schmar (2021) calculates that fraud can cost banks as much as five per cent of annual revenue. In response, many jurisdictions have adopted technological innovations to improve financial crime prevention, including Machine Learning (ML), Artificial Intelligence (AI), RegTech solutions, and blockchain for transaction monitoring (Arner, Barberis, & Buckley, 2017; FATF, 2021). These technologies enable institutions to automatically flag suspected transactions, enhance customer due diligence and thereby meet AML compliance standards.

These technologies have been highlighted by international regulators as a mandatory necessity. Financial Action Task Force (FATF, 2021) encourages member states to adopt technology in the fight against money laundering and the financing of terrorism (ML/TF) to strengthen monitoring and surveillance. The first world countries have moved towards applying these technologies in anticipation of and with the aim to bridge the gap between regulatory requirements and advanced technological infrastructure. However, the critical problem that emerges from the global experience is not whether technology is being adopted, it is whether technology adoption is translating into measurable crime prevention outcome or whether it is merely satisfying regulatory requirements without meaningfully reducing financial crime. This distinction between technology as a compliance tool and technology as an effective crime prevention instrument is the fundamental problem that motivates this study.

Southern African Context

Zimbabwe's financial crime challenge cannot be examined in isolation, as it forms part of a wider systemic crisis that pervades the Southern African Development Community (SADC) problem is not a product of isolated institutional failure it is part of a wider pattern of systemic weakness in financial crime prevention across Southern Africa. Financial crime constitutes the most prevalent category of criminal activity reported across SADC member states, representing 43% of all recorded crime in the region and encompassing offences such as bank fraud, money laundering, credit card skimming and cyber-enabled financial theft (SARPPCO, 2022). The collective fiscal impact on member states is considerable, with billions of United States dollars lost annually to illicit financial flows facilitated by transnational organised crime networks. The Institute for Security Studies (ISS, 2023) further establishes that Zimbabwe features among the highest-ranked

countries on the African Organised Crime Index, alongside South Africa and the Democratic Republic of Congo. This regional positioning is analytically significant, as it situates Zimbabwe's financial crime problem not as an aberration of individual institutional weakness, but rather as a manifestation of entrenched structural deficiencies in financial crime prevention that are characteristic of the broader Southern African sub-region.

Of particular relevance to this study is the pronounced inequality in the technological capacity of SADC member states to respond to the financial crime threat. South Africa, as the most economically advanced financial system in the region, sustained financial crime losses amounting to R3.3 billion in 2023, accompanied by a 45% escalation in digital banking fraud during the same period (SABRIC, 2024). Notwithstanding these losses, South Africa's banking sector has demonstrated measurable advancement in the deployment of AI-driven fraud detection frameworks, biometric authentication mechanisms and sophisticated AML compliance technologies. Zimbabwe, however, has not attained a comparable level of technological maturity in its financial crime prevention infrastructure. The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG, 2023) has determined that Zimbabwe, together with a number of other SADC member states, remains substantially non-compliant with FATF recommendations on AML/CFT effectiveness. The principal impediments identified include chronically underfunded financial intelligence units, an excessive reliance on rule-based transaction monitoring systems and a pronounced lack of operational coordination between banking institutions and national law enforcement authorities. This assessment is corroborated by Chitimira (2021), who observes that whereas South Africa has commenced the integration of artificial intelligence into its AML operational frameworks, Zimbabwe and comparable neighbouring jurisdictions remain dependent on first-generation, reactive compliance mechanisms that are fundamentally inadequate for detecting the increasingly sophisticated financial crime typologies prevalent in the region.

Zimbabwean Context

The Zimbabwean financial system is evolving quickly with the adoption of electronic banking and mobile money for transactions. According to the RBZ, 2023, mobile banking and RTGS systems have become the preferred choice for payments within the country, a development attributable to Zimbabwe's push towards a cashless economy as well as the quest for financial inclusion. It should

be noted that the implementation of sophisticated technology-based countermeasures in Zimbabwe is lagging behind the best practices in the rest of the world. Cases of cyber-based financial crimes such as phishing, SIM swapping, and mobile banking fraud have grown proportionately with the growth of the adoption of technology (Tachiona, 2020; Mashizha & Kanengoni, 2024).

In 2023 CBZ Holding annual report highlighted how the bank had automated transaction monitoring systems in place to detect any suspicious transactions and prevent any form of fraudulent transactions. Despite having such advanced technologies, the bank noted that there was an increase in some forms of cybercrime, especially on the mobile banking platform, indicating how it is difficult to keep up with the advancement in digital fraud schemes (CBZ Holdings, 2023). The same was witnessed in FBC Holdings Limited, when in 2022 the bank experienced a major cyber-enabled fraud attack where a phishing attack led to considerable financial loss of corporate clients. To prevent such attacks in future, the bank enhanced its fraud detection system by adopting machine learning algorithms (FBC Holdings, 2023).

Even though automation technologies have been adopted in these financial organisations, the continued existence of financial crime leads to the emergence of important concerns regarding the assumptions of prevention based on technology. In particular, rule-based prevention systems are mainly used in Zimbabwean banks. As noted by Arner, Barberis and Buckley (2017), rule-based systems struggle to keep pace with constantly evolving financial crime tactics, making them less effective over time. This indicates that not only is the adoption of technological innovations important, but also the type of innovation and its ability to learn should be considered. The use of the first generation of AML modules in Zimbabwe, as opposed to AI-based innovations used in developed countries, may partially answer the question posed above.

In accordance with the Financial Intelligence Unit Zimbabwe (FIUZ) directive for all banks to have automated transaction monitoring system under the authority of RBZ, Zimbabwean banks have filed 1,247 Suspicious Transaction Reports (STRs) in 2023, a fifteen percent increase compared to 2022 (FIUZ Annual Report, 2023). Unfortunately, only twenty-three percent of the reports were investigated by law enforcement agencies, implying high false positives or poor implementation of follow-up procedures. In addition, the total financial crime loss suffered by the country in 2023 was estimated at more than ZWL\$2.5 billion by the Zimbabwe Republic Police

(ZRP, 2024). It clearly shows the inability of technology to prevent criminal activity within the country (FIU Zimbabwe, 2023; Business Daily News Zimbabwe, 2025).

However, laws such as the Money Laundering and Proceeds of Crime Act [Chapter 9:24] (Zimbabwe, 2013) and the Cyber and Data Protection Act [Chapter 12:07] (Zimbabwe, 2021) can serve as legislative guidelines for anti-money laundering regulations, but enforcement issues continue to exist. Several academic studies highlight this issue. An instance in point is the fact that, according to Chitimira (2021), the technological tools used by Zimbabwean banks for detecting fraud transactions are reactive as opposed to being proactive and relying on AI technologies as applied by advanced banking systems. Likewise, Jimu and Chimwai (2025) emphasise the importance of financial intelligence units in analysing transactions and ensuring regulatory compliance.

Some differences on the extent to which international best practices are applied and to the Zimbabwean context are as follows: while AI and machine learning technology is applied in international best practices, rule-based transaction monitoring are used in the Zimbabwean scenario. Proactive risk identification is employed in the international practice and the Zimbabwe case is reactive compliance reporting. While false positive rate is very low in the international practice, the false positive rate in Zimbabwe is higher leading to alert fatigue. Sharing of data with FIU occurs via real-time data feeds internationally and via manual and inconsistent STR submissions in the Zimbabwe context. Internationally, there has been a shift from compliance-based practices to outcome-based effectiveness, while in Zimbabwe, the practice is still compliance-based.

The issue of adoption versus implementation of technology in Zimbabwe can be analysed using the concepts of the two theories. Even though the banks in Zimbabwe have adopted AML technologies, their usefulness may not go beyond just complying with regulations but detecting financial crimes. Moreover, the use of the latest technology driven by AI is hindered by factors such as cost, skill and infrastructure, which explains the inability of the Zimbabwean banks to adopt any other system apart from the rule-based system.

Although the existing literature suggests that AML technology has been adopted by the banks of Zimbabwe, it does not justify why financial crime continues despite such efforts. There is no empirical evidence of the effectiveness of existing technology for detecting financial crime, the

impact of false positives on the efficiency of compliance or what factors influence the transition from rules-based to intelligent system-based compliance management. The relationship between international technological progress and the environment of Zimbabwean banking highlights a crucial knowledge gap, given that even though international standards can act as benchmarks, the local conditions might not reflect it

The convergence of global technological progress and Zimbabwean banking problems underscores a critical gap: even though international norms promote the use of intelligent systems and proactive techniques for financial crime detection, Zimbabwean banks are struggling with rules-based systems, scarce resources and a reactive compliance culture. The gap is not just technological, but systemic- it reflects issues of regulation, human competence and coordination. Therefore, ascertaining the effectiveness of existing technologies is essential to address the gap. The study seeks to do just that by providing empirical findings on the nature, effectiveness and challenges of existing technology in Zimbabwean banks.

1.2 Problem Statement

Despite investments in Anti-Money Laundering technologies, Zimbabwe's banking sector continues to experience financial crime incidents raising concerns about the effectiveness of these technologies in preventing and detecting financial crime. Investments have been made in banking systems with embedded AML modules due to a high-risk operating environment caused by currency shortages and the prevalence of cross-border informality. These systems do not seem to have moved beyond just being tools of compliance, in the fact that they do not act as detection tools, as financial crime still occurs even after investing in such systems. It can be identified that the underlying problem is the lack of empirical research on how such technologies actually work in Zimbabwe; banks are making use of rule-based systems, and the effect of rule-based systems is a high number of false positives and alarm fatigue, while the linkages between bank detection systems and national financial intelligence mechanisms is largely unknown. This research is therefore needed, because if technology effectiveness is not empirically assessed, the relevant policymakers and bank executives may implement solutions, whose contribution to crime prevention is unknown; leaving Zimbabwe to suffer continuing losses from financial crimes and sanctions due to AML/CFT deficiencies.

1.3 Purpose of the Study

This aims to provide a critique on how digital technology is being used in the detection and prevention of financial crime in the banking sector of Zimbabwe. It will determine the tools that are being used, and will evaluate how effectively these are working and will develop an integrated technological financial intelligence sharing framework among the banking institutions and regulatory authorities.

1.4 Objectives of the Study

The objectives of the study are as follows:

1. To identify the financial crime prevention technologies currently used by commercial banks in Zimbabwe.
2. To assess the effectiveness of these technologies in identifying and reporting suspicious transactions to the Financial Intelligence Unit of Zimbabwe.
3. To investigate the technical, financial and human capital challenges that impede the optimal use of financial crime prevention technologies in Zimbabwean banks.
4. To recommend strategies for improving the adoption of emerging technologies in financial crime prevention within Zimbabwean banks.

1.5 Research Questions

To achieve the above objectives, the study will address the following questions:

1. Which financial crime prevention technologies are currently used by commercial banks in Zimbabwe?
2. How effective are these technologies in identifying and reporting suspicious transactions to the Financial Intelligence Unit of Zimbabwe?
3. What technical, financial and human capital challenges impede the optimal use of financial crime prevention technologies in Zimbabwean banks?
4. What strategies can be recommended to improve the adoption of emerging technologies in financial crime prevention within Zimbabwean banks?

1.6 Significance of the Study

The following stakeholders will benefit from this study:

1.6.1 To the researcher

The knowledge that the researcher possesses regarding the link between technology and financial crime prevention in the banking sector of Zimbabwe will be greatly enhanced through this study. This study will provide the student with practical experience in analysing data and conducting empirical research. The findings of this study will assist the researcher to progress academically and form the basis for future studies in this field.

1.6.2 Policy Makers (RBZ and FIUZ)

The results of the study will generate empirical data on the real performance of the technology used for financial crime detection, hence allowing the Reserve Bank of Zimbabwe and FIUZ to develop an outcome-based AML/CFT regulatory framework.

1.6.3 Banking Institutions

The commercial banks will be able to gain knowledge on how the different technologies compare in terms of effectiveness, thus enabling the Chief Risk Officer and the Head of Compliance to make an informed decision on the investments to make.

1.6.4 Academia and Future Researchers

The research work will add to the existing literature on the prevention of financial crimes in Zimbabwe, especially that in the Bindura University e-Scholar collection, and offer a basis for future research into the relationship between information technology and financial criminology.

1.7 Assumptions of the Study

Respondents are assumed to be truthful in their answers regarding their experience with financial crime prevention technologies. The data collection instruments are assumed to be valid and reliable in measuring the intended constructs. It is further assumed that respondents possess sufficient familiarity with the technologies used in their respective institutions to answer the questions appropriately. Finally, the sample is assumed to include a broad cross-section of large commercial banks in the Zimbabwean banking sector, and the institutional contexts of the two banks are

assumed to have remained sufficiently stable during the data collection period to enable meaningful cross-case comparison.

1.8 Delimitations of the Study

Geographical Region: The research will be restricted to the banking sector in Harare, Zimbabwe, which is the head office of the leading commercial banks, where both compliance and IT departments have their central location.

Conceptual Scope: The study is subject to prevention and detection technologies. It also makes no mention of the legal prosecution of financial crime and briefly mentions non-bank-related fraud like insurance or micro-lending fraud.

Population Scope: The population of study will be compliance officers, IT security managers and internal auditors of sampled commercial banks. The primary data sample does not include general bank clients and law enforcement officers.

Time Horizon: The study is cross-sectional because the information is mainly collected during the years 2020-2024, a time period when there was a high level of digital adoption after COVID-19.

Variable Scope: Technological adoption is considered as an independent variable, and the effectiveness of financial crime prevention is the dependent variable.

1.9 Limitations of the Study

Theoretical and Measurement Limitations

Theoretical frameworks (Diffusion of Innovations and Technology Acceptance Model) might not fully capture technology adoption in the Zimbabwean banking context. As a solution to this problem, the researcher will be willing to accept qualitative results that do not conform to the theory. While the surveys might not include all constructs of interest, a pilot study among compliance officers will be undertaken.

Design and Sampling Limitations

The mixed-methods case study approach may not fully address the complexities surrounding the application of technology by all banks. Triangulation of data using surveys, interviews, and

documentation will be used to enhance the validity. The results obtained may not be generalised for all banks in Zimbabwe, but purposive sampling will ensure representation within the scope of the research.

Data Quality and Temporal Limitations

The respondents may give subjective or even incomplete information. Anonymity and confidentiality will be assured, and neutral interviewing techniques will be used in order to ensure that the respondents answer their questions honestly. While the cross-sectional approach cannot account for any changes, the data will be collected very quickly so that the effect of any changes in regulations or technology will be minimised.

1.10 Definition of Terms

The following were operationally defined for clarity and consistency:

Financial Crime: Illegal acts committed for financial gain, including money laundering, mobile banking fraud, and cyber-enabled forgery reported to the FIUZ (FIUZ, 2022).

Anti-Money Laundering (AML): The policies, laws, and procedures designed to prevent criminals from concealing illegally, criminally obtained funds as legitimate income (Financial Action Task Force, 2021).

RegTech (Regulatory Technology): The application of technology to enhance regulatory and compliance processes within financial institutions (Arner, Barberis & Buckley, 2017)

Suspicious Transaction Report (STR): It's a report submitted by financial institutions to the FIUZ regarding transactions suspected to involve illegal activity or money laundering (Financial Intelligence Unit of Zimbabwe, 2022).

Financial Intelligence Unit of Zimbabwe (FIUZ): The National Authority for the reception and treatment of the information and analysis related to financial intelligence on money laundering and terrorist financing (Reserve Bank of Zimbabwe, 2020).

Artificial Intelligence / Machine Learning (AI/ML): A sub-field of artificial intelligence which uses computational processes that allow computer systems to automatically learn from and adapt

to the new information without manual programming, is often used for identifying the patterns which might betray financial crime (Arner, Barberis & Buckley, 2019).

False Positive: An alert generated by a monitoring system that flags legitimate activity as suspicious, contributing to inefficiency and alert fatigue (Dube & Ndlovu, 2023).

Customer Due Diligence (CDD): The process of identifying customers, assessing their risk profiles, and monitoring account activity to detect unusual transactions (Financial Action Task Force, 2021).

Technology Acceptance Model (TAM):

This is framework that predicts user acceptance of technology based on perceived usefulness and perceived simplified use (Davis, 1989).

Diffusion of Innovations: A theory explaining how, why, and at what rate new ideas and technologies spread through social systems (Rogers, 1995).

1.10 Dissertation outline

This dissertation is structured into five chapters. Chapter One introduces the background, problem statement, objectives and significance of the study. Chapter Two reviews relevant literature, covering conceptual and theoretical frameworks as well as empirical evidence from global, African and Zimbabwean contexts. Chapter Three details the research methodology, including the research design, sampling, data collection and analysis techniques. Chapter Four presents the analysis and interpretation of data collected from questionnaires and semi-structured interviews at CBZ Holdings and FBC Holdings. Chapter Five concludes the study with a summary of findings, conclusions and recommendations for both practice and future research.

1.11 Chapter Summary

This chapter has established the foundation for the research that seeks to investigate the role of technology in financial crime prevention in our banking sector. From the background discussion, it can be noted that there exists a critical mismatch between the international trends in terms of

technology adoption and the realities of Zimbabwe's banking industry. This has been identified as the central research problem to be investigated in this study. Purpose, objectives and research questions have been clearly stated. The significance of the research has also been stated for the relevant stakeholders. Delimitations and limitations have also been clearly stated together with their respective mitigation measures. Lastly, operational definition of terms were established for consistency in usage of all terms and concepts throughout this study. Next chapter is literature review regarding financial crime, technologies to address crime, theoretical issues and research findings that are international and within Zimbabwe.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The chapter discusses theoretical basis underpinning this study regarding the role of technology in fight against financial crimes in Zimbabwean banking industry in depth. After discussing theoretical base, a conceptual model was designed illustrating the interaction of the central theoretical constructs, and their use in relation to this study context. The research will discuss empirical work as a follow up, relating evidence and the study research questions and discussing research gaps, before ending the chapter with a summary.

2.1 Conceptual Framework

Conceptual framework is the system that is used to organise main concept of research and show the relationship among them (Creswell, 2014). According to Creswell (2014) A conceptual framework is a visual and, often, heuristic device for organizing theoretical concepts and variable and providing the theoretical linkage among them.

2.1.1 Conceptualising Financial Crime

Financial crime encompasses illegal acts committed for financial gain, including money laundering, fraud, cybercrime and terrorist financing. In their study, Ferwerda, Deleanu and Unger (2021) explain that money laundering involves concealing the traces of means used to obtain the illegally obtained funds. Money laundering is the act of concealing or disguising the proceeds of illegal transactions to give them a legitimate appearance. Financial fraud comprises identity fraud, phishing, unauthorised online money transfer, and mobile banking fraud. The above definition of financial crimes is confirmed by Manhida and Nkomo (2024), who state that the forms of fraud highlighted above are common among Zimbabwean banking systems.

In Zimbabwe, the legal measures to fight financial crimes include the Money Laundering and Proceeds of Crime Act [Chapter 9:24] and the Cyber and Data Protection Act [Chapter 12:07]. These are according to the findings made by Zimbabwe (2013) and Zimbabwe (2021). According

to the Financial Intelligence Unit of Zimbabwe (2023), mobile banking fraud, SIM card swapping fraud, and phishing attacks are the most common financial crimes in Zimbabwean banks.

2.1.2 Technological Solutions for Financial Crime Prevention

Rule-Based Versus AI-Driven Systems

An important contradiction has been identified through the literature concerning the efficiency of different types of technological techniques. According to Arner, Barberis and Buckley (2017), rule-based systems use threshold values to alert, but such systems yield high rates of false positives. The above contradiction implies that even though Zimbabwean banks have incorporated rule-based systems to a great extent, as stated by Dube and Ndlovu (2023), the banks may be using technology that is less efficient than that used by their international counterparts. Nevertheless, there is no evidence in existing literature on whether the efficiency of AI-based systems will hold true in Zimbabwe.

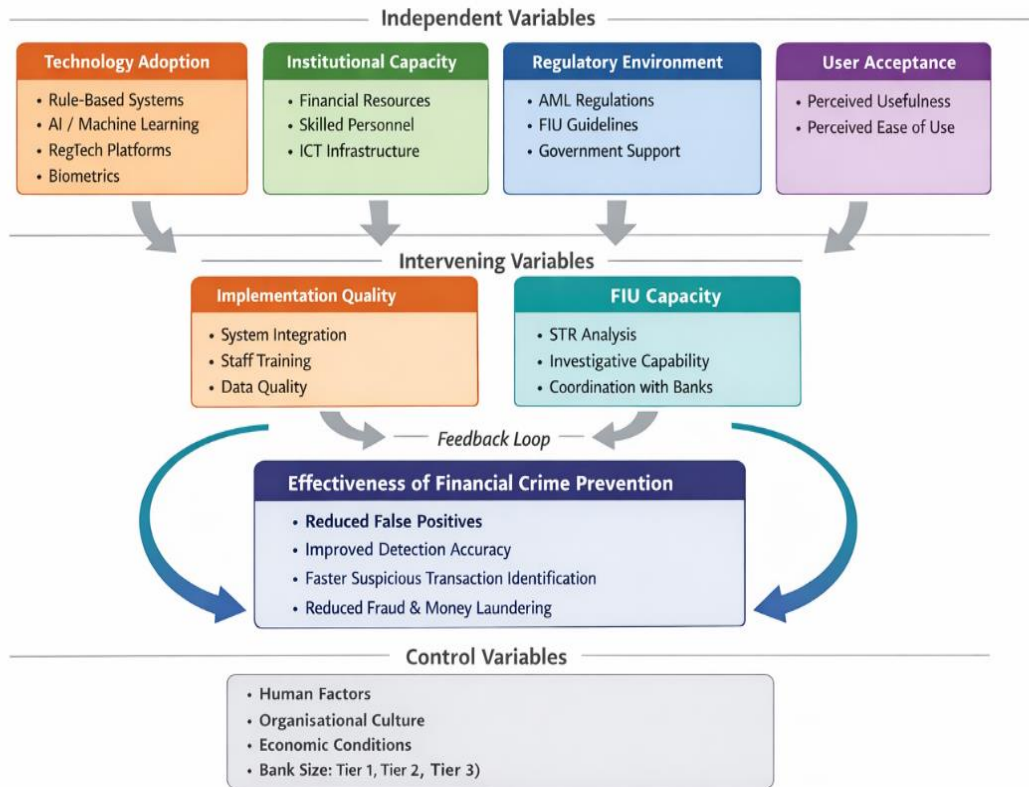
RegTech, Biometrics and Blockchain

Arner et al. (2017) suggest that RegTech helps ease compliance processes and eliminate manual errors. Nonetheless, the Financial Intelligence Unit of Zimbabwe (2023) shows that RegTech is still in its infancy stage in Zimbabwe since most banks still conduct their operations manually. Biometrics, according to Manhida and Nkomo (2024), is used as a means of customer due diligence instead of a transaction monitoring technique since its adoption is only within selected banks for account opening purposes. Arner et al. (2019) claim that blockchain can be used to ensure transparency of transactions. On the contrary, some findings have shown that blockchain is yet to be adopted in Zimbabwe due to several challenges, as per Dube and Ndlovu (2023) and Reserve Bank of Zimbabwe (2023).

2.1.3 Classification of Technologies

Table 1: Classification of Financial Crime Prevention Technologies

Technology	Primary Function	Adoption Status in Zimbabwe	Source
Rule-Based Systems	Transaction monitoring, alert generation	Widely adopted	Dube & Ndlovu (2023:58)
AI/ML Solutions	Adaptive detection, predictive analytics	Not adopted	Chitimira (2021:15)
RegTech Platforms	Automated reporting, customer due diligence	Limited adoption	Dube & Ndlovu (2023:60)
Biometrics	Customer identification, authentication	Selected banks (account opening)	Manhide & Nkomo (2024:52)
Blockchain	Transaction traceability	Not adopted	RBZ (2023:45)



Theoretical Basis: Diffusion of Innovations (Rogers, 1995) & Technology Acceptance Model (Davis, 1989)

Figure 1: Conceptual Framework for The Role of Financial Crime Prevention in Zimbabwe's Banking Sector

As seen from the above framework, technology adoption, institutional capability, regulation, and user acceptance have an impact on implementation capability and FIU capability, which in turn affect prevention capability. The control variables will be moderating all relationships, and there will be a feedback loop for improvement.

2.3 Theoretical Framework

The importance of theory in any investigation may be characterised by three significant roles: they may explain the observations from an empirical study, they are able to offer some predictions of

what the outcome will be, and provide for the organization of prior research. Given this framework, this study is built upon two highly relevant theoretical models, which served as a foundation for this research, the diffusion of innovation theory and the technology acceptance model.

2.3.1 Diffusion of Innovations Theory

Rogers (1995) developed the Diffusion of Innovations Theory to explain how and why new technologies are adopted and spread within social systems over time. The theory lists five attributes that influence rate of adoption: relative advantage, compatibility, complexity, trialability and observability. Rogers (1995) also classifies the adopters into five categories innovators, early adopters, early majority, late majority and laggards, each with a different attitude towards the adoption of new technologies.

The theory is important in the current study as it provides an understanding of why Zimbabwean banks have embraced rule-based AML systems but have been slow to adopt more advanced AI-Driven systems. In combination, the high complexity of AI systems, high capital cost of these systems, low trialability and low observability of outcomes continue to make the sector reliant on first-generation of compliance tools (Dube & Ndlovu, 2023; Chitimira, 2021). The theory connects directly to the goals of the study as it guides the identification of technologies in use, positioning Zimbabwe's banking sector on the technology adoption continuum, it explains the technical, financial and human capital challenges by the attributes of complexity, compatibility and trialability, and provides a basis for recommending technologies to enhance their adoption of advanced technologies. The theory's major advantage is its ability to not only consider whether technology has been adopted or not, but also what makes it adoptable or not a concept that is important to this study. The theory has been criticized, however, as being pro-innovation and not considering rational non-adoption due to resource constraints, which is relevant in Zimbabwe's economic environment (Dube & Ndlovu, 2023).

2.3.2 Technology Acceptance Model

Davis (1989) proposed the technology acceptance model (TAM) to explain how individual users adopt and accept technology. The model is based on two basic constructs, perceived usefulness, belief that using a technology improves a user's job performance and perceived ease of use, belief that a technology is easy to use. Together, these two constructs explain a user's attitude towards and actual use of a specific technology (Davis, 1989).

It is important to this study because it helps explain why AML technologies may not achieve their intended effectiveness despite being adopted by banks. The model serves as a theoretical lens to analyse the key difference between technology adoption (as an institutional decision) and technology acceptance (as a behavioural reality). Compliance officers regard rule-based systems as beneficial tools to ensure regulatory compliance but not to detect financial crimes, undermining the financial crime prevention function of these tools (Chitimira, 2021). Manhide and Nkomo also point out that complex interfaces and poor staff training seriously hinder perceived ease of use. TAM contributes to the study objectives by informing the assessment of technology effectiveness through user perception, identifying human capital challenges that hinder optimal technological use and providing a basis for recommending interventions that improve perceived usefulness and ease of use among compliance personnel. The key strength of TAM is that it reveals that institutional adoption does not necessarily translate into effective individual utilisation, a distinction that is critical in understanding in Zimbabwe's operational challenges in financial crime prevention. However, in Zimbabwean banks, compliance officers are required to use AML systems regardless of their perceptions of the technology's usefulness, whereas TAM assumes that technology use is voluntary (Jimu & Chimwai, 2025; Taherdoost, 2018).

2.3.3 Integration of Theories

The study combines both theories to present a holistic framework. Rogers (1995) noted that diffusion theory provides an explanation for how organisations adopt new technologies, and Davis (1989) suggested that the Technology Acceptance Model accounts for the users' acceptance of new technologies. Both of the theories, however, do not explicitly refer to FIU capacity, and the study must be extended to the Zimbabwean economic context.

The current study presents an expanded Integrated Framework that includes additional contextual elements that were not addressed in the original theories. First, FIU capacity is introduced as a mediating variable because the effectiveness of the implementation of technology in banks relies on the analytical and investigative capability of Financial Intelligence Unit of Zimbabwe which processes Suspicious Transaction Reports. Secondly, economic context (foreign currency shortages, inflationary pressure, constraints on infrastructure), is controlled for on the basis that these factors will affect technology adoption, maintenance and the retention of personnel in Zimbabwean banks. This addition is not in opposition to the theories but an adaptation of the theories to the context of Zimbabwean banks, "as advised by literature for the contextualization of technology adoption models in developing countries (Chitimira, Dube & Ndlovu, 2023)." The reason both theories are applicable in this context is that they explain why the banks in Zimbabwe have opted for rule-based systems and not AI systems. This can be attributed to Rogers (1995), Davis (1989) and Jimu & Chimwai (2025), who prove that the entire chain of organisational adoption and user acceptance addresses the research problem directly.

2.4 Empirical Evidence

This paper takes a top-down approach beginning with international research before narrowing down to African research, finally focusing on Zimbabwean research.

2.4.1 Global Studies

The literature at international level shows clear evidence on the benefits of AI based systems over rule-based systems. In the eyes of Arner, et al (2017), the utilisation of RegTech could lead to reduced compliance costs and more efficient reporting processes. Further expanding on their analysis, Arner, Barberis and Buckley (2019) highlight that blockchain and distributed ledger technology provide more applications in transaction monitoring and identity management.

The Financial Action Task Force (2021) gives some case studies from the UK, Singapore and the USA, indicating that AI-powered transaction monitoring has helped in detecting money laundering activities. However, the Financial Action Task Force (2022) warns that while adopting new technologies, an effective governance framework should also be adopted to avoid algorithmic bias.

This warning is important in the case of Zimbabwe since there are no governance frameworks for AI in Zimbabwe.

According to Ferwerda et al. (2021), rule-based static models cannot cope with innovative crime, making the use of artificial intelligence a necessity. This is corroborated by United Nations Office on Drugs and Crime (2022), which asserts that digital financial platforms have made the process of detecting illicit financial flows more difficult due to their enhanced speed and scope.

2.4.2 African Studies

Not all African countries have achieved the same outcomes. As Chitimira (2021) pointed out, the use of AI in Anti Money Laundering (AML) systems is further developed in South Africa compared to other Southern African countries such as Zimbabwe, Zambia and Botswana. However, this same researcher contends that the diffusion of technologies is held back by lack of infrastructure, lack of skills and lack of coherent regulation.

Here, there is contradiction among researches as while Chitimira (2021) blames infrastructure challenges as primary reasons for adoption, Manhide and Nkomo (2024) blames human capital and cybersecurity. Using the quantitative survey approach, Manhide and Nkomo (2024) observe that lack of customer awareness and poor fraud detection mechanisms are key determinants of persistent banking fraud. Hence, the barriers are many and interact, and hence, single-barrier explanations do not suffice.

In addition, Mashizha and Kanengoni (2024) use a mixed methods approach to investigate the adequacy of cybersecurity in Zimbabwean financial institutions. The researchers find that most banks do not have good intrusion detection, incident response mechanisms, and security audits. According to Mashizha and Kanengoni (2024), infrastructure shortcomings such as poor power and internet connections also undermine cybersecurity efforts.

2.4.3 Zimbabwean Studies

The research conducted by Zimbabwean researchers in the field of financial crime prevention technologies is still developing and underdeveloped. Dube and Ndlovu (2023) study the difficulties of adopting RegTechs in Tier 1 banks by conducting qualitative interviews with compliance

officers and IT managers in banks. In their work, the authors single out the costliness of the technology adoption process, lack of skills, and regulatory uncertainty as the main obstacles to adopting new technologies. It is noteworthy that, according to Dube and Ndlovu (2023), the rate of false positives in Zimbabwean banks exceeds eighty per cent, which causes alert fatigue and lowers the efficiency of compliance.

Jimu and Chimwai (2025) considered Financial Intelligence Unit of Zimbabwe's roles in fighting money laundering based on the recommendations of the Financial Action Task Force. As a result of the analysis, it was found that the number of Suspicious Transaction Reports submitted to the FIUZ is growing, but the unit does not have enough resources to conduct thorough investigations. According to Jimu and Chimwai (2025), the authors suggest that the problem of data analysis must be solved.

In a legal analysis of financial crime enforcement in Zimbabwe, Chitimira (2021) argues that most of our regulatory frameworks are lagging behind on technological change. The author calls for legislative reforms to mandate AI-driven monitoring systems and enhance penalties for non-compliance.

A single case study by Gutsa (2024) reports a ninety-five per cent increase in fraud detection at CBZ Bank following the implementation of data analytics and machine learning algorithms. However, this finding should be treated with caution, as it is based on self-reported data from one institution and may not be representative of the broader banking sector.

2.5 Research Gap

Unfortunately, the body of literature in this research topic, "the role of technology in the fight against financial crime," is limited. Zimbabwe's banking sector's case study demonstrates a number of research areas which may require more attention and include the following;

While Zimbabwean studies confirm that banks have adopted AML technologies (Dube & Ndlovu, 2023), no empirical research has assessed the actual effectiveness of these technologies in detecting illicit activity. The relationship between technology adoption and crime reduction outcomes remains unexplored. Dube and Ndlovu (2023) discuss problems faced during the adoption process, but they fail to determine the extent to which the adopted technology can help

identify any criminal activity. As such, there is inadequate information to guide decision-making in terms of technology investments.

The effects of the high false positive rate on the efficiency of compliance within banks in Zimbabwe have not yet been determined. Although Dube and Ndlovu (2023) indicate that false positive rates exceed eighty percent, the implication of this trend in terms of resource allocation for compliance officers, investigation effectiveness, and the failure to capture actual instances of suspicious activities has not yet been established. Several international studies indicate that false positive rates reduce effectiveness, but there are no specific figures for Zimbabwe.

The factors that prevent transition from rules to AI have not been analysed comprehensively. Although issues such as costs and skills have been discussed in other studies, there is no analysis that covers all the factors involved. Other research findings have highlighted individual barriers (Chitimira, Manhida & Nkomo, 2024).

The link between the effectiveness of technology-based systems at the level of banks and the analytical capability of the FIU is not well researched. Jimu and Chimwai (2025) look at the ability of FIUZ but fail to relate it to the efficacy of the technology-based system at the banks. How Suspicious Transaction Reports lead to investigations and prosecutions needs empirical research.

Theoretical application of Diffusion of Innovations and TAM to the banking industry in Zimbabwe has not been conducted. Earlier research has not empirically tested how perceived usefulness, compatibility, and complexity affect the outcome of technology adoption in banks in Zimbabwe. The integrated theoretical framework in this research has not been applied to the banking industry of Zimbabwe before.

Blockchain and artificial intelligence/machine learning (AI/ML) are popularly used terminologies in the global literature as advanced solutions to the problem of AML, but there is no study that looks at their adoption in the Zimbabwean banking context. While acknowledging these technologies as emergent technologies beyond the current scope of empirical research, they have been included in the theoretical framework.

There has been no study assessing the efficacy of technological tools used in preventing financial crimes in all levels of banks in Zimbabwe, from Tier 1 to Tier 3 banks. Studies have concentrated on the use of such tools in Tier 1 banks (Dube & Ndlovu, 2023).

2.6 Chapter Summary

The chapter has looked at the literature reviewed on technological innovations for financial crime prevention, theories, and empirical evidence. The development of financial crime has been necessitated by digitalization, thus the need for sophisticated technological innovation, but the rule-based systems that have dominated the banking industry in Zimbabwe have produced a false positive rate that exceeds eighty percent. The theoretical framework encompasses two theories which explains organizational and individual adoption of technological innovations respectively, although each theory has some limitation in the Zimbabwean context. Empirical evidence indicates that AI technology has improved the performance of systems in terms of reducing false positives globally, while African literature points out infrastructural weaknesses and lack of regulation as barriers to adoption, despite contradicting findings about whether infrastructure or human resource constitutes the main barrier. However, there is no research on technology adoption in Zimbabwe.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter describes the research methodology which was used to examine the effect of technological intervention on prevention and detection of financial fraud within Zimbabwe's banking sector focusing on CBZ Holdings and FBC Holdings. This section gives a full description on the design of the research, population dimensions, sample size and sample techniques of collection, study tools, tests of trial or pilotage of the tools, measure of validity and reliability of the tools, technique of collecting data, methods of analysing data, ethics to be followed and limits of study. It is expected that through this chapter, we clearly explain the methodology used to capture required data that are related to objectives of this study.

3.1 Research Philosophy

Research philosophy refers to the system of beliefs and assumptions that guide how knowledge is gathered, interpreted and used in a study (Saunders, Lewis & Thornhill, 2019). This study followed a pragmatist research philosophy. Pragmatism assumes that research should focus on outcomes rather than on philosophical stances (Creswell & Creswell, 2023). According to Morgan (2014), pragmatism provides a practical and action-oriented paradigm for social research by emphasising the relationship between knowledge and action. In the context of mixed methods study, the philosophy of this research is relevant as researcher can implement both the quantitative and qualitative methodologies based on the types of questions asked. Unlike positivism which holds the view of single objective reality and interpretivism which emphasises on subjective meaning, pragmatism is able to accept multiple realities that can exist at the same time and that the selection of research methods should be guided by their usefulness in addressing the research problem (Kumar, 2019). The pragmatist philosophy therefore justified the integration of quantitative data (to measure technology adoption and effectiveness) with qualitative data (to understand participant experiences and institutional challenges), as neither quantitative nor qualitative data alone could provide a complete answer to the research questions.

3.2 Research Approach

This study adopted an abductive research approach. Saunders, Lewis and Thornhill (2019) have explained that abduction is a process that involves switching back and forth between theory and data, starting from an observation of a phenomenon, formulating a temporary theory, and then refining the theory through further empirical study. Abduction differs from deduction, which focuses on testing existing theory, and from induction, which focuses on developing theory from data. Instead, it combines elements of both approaches by testing existing theory while allowing new theoretical insights to emerge from the data. This approach was suitable for the current study because it enabled the researcher to use existing theories as preliminary explanatory frameworks while allowing field observations to refine and extend those theories within the context of Zimbabwe's banking industry.

3.3 Research Design

Research design refers to the overall strategy and plan that guides the collection, measurement and analysis of data in order to address the research questions of the study (Creswell & Creswell, 2023). In the context of mixed methods study, the philosophy of this research is relevant as researcher can implement both the quantitative and qualitative methodologies based on the types of questions asked. with a case study approach. According to Creswell and Creswell (2023), a convergent parallel research design collects quantitative and qualitative data, analyses each data type independently, and combines the results in interpreting the data. This design was suitable for this study because the researcher gathered the data in both surveys and interviews in the same time frame, analysed each independently by descriptive statistics and thematic analysis and then compared the results for convergence and divergence.

In an attempt to provide an overall explanation for a specific research problem, one study used a combined quantitative/qualitative research methods design. Given the need to combine quantitative measures (to identify patterns and consensus level) and qualitative explanations, this approach was suitable to this study. Creswell and Creswell (2023) argue that mixed methods

studies are suitable when a researcher needs to have breadth as well as depth of information on a specific topic.

One advantage of the design is that the researcher could combine the advantages of quantitative and qualitative approaches. The quantitative data provided breadth, in that they provided an overall trend and level of consensus, and the qualitative data provided depth, in that they provided explanations for the overall trend observed. The second advantage is that the design improved triangulation as results obtained from the first method could be compared to the results obtained from the second method, thus enhancing the reliability of this study. Both approaches were used, and as Creswell and Creswell (2023) noted, the combination of the two approaches reduced the weaknesses of either, and improved the quality of the analysis.

The case study method was also suitable since it enabled the researcher to analyse the problem in the context of the real banking world. A case study proved to be appropriate in circumstances where research sought to investigate a current issue. It provides a comprehensive grasp of the phenomenon under investigation, particularly when the researcher is interested in learning more about the use of technology in institutions. This research adopted the case study method which helped the researcher to understand the deployment of the technology by each firm in the battle against financial crimes in CBZ Holdings and FBC Holdings.

3.4 Study Population

The sample for the study consisted of employees in CBZ Holdings and FBC Holdings involved in the prevention of financial crimes. The participants were mostly those who worked in areas of compliance, internal auditing, and IT/Security, since they were expected to have prior knowledge regarding the technology used in detecting current and preventing future financial crimes. In this sense, the population of this study is appropriate, as the opinions regarding the technologies analysed must be informed and come from the population that have had some experience with such technologies. According to Kumar (2019), the study population should include the people from whom data could be solicited concerning the research problem.

3.5 Sample size and Sampling Techniques

In this research, 60 participants were involved. Amongst them, 50 respondents took part in the questionnaire survey, where 25 were from CBZ Holdings, while 25 others were from FBC Holdings. In addition, 10 participants were involved in the semi-structured interviews, 5 from each bank.

Table 2: Sample Constituency

Department	CBZ Holdings (Questionnaire)	FBC Holdings (Questionnaire)	CBZ Holdings (Interview)	FBC Holdings (Interview)	Total
Compliance	10	10	2	2	24
Internal Audit	8	8	2	2	20
IT/Security	7	7	1	1	16
Total	25	25	5	5	60

Regarding the quantity aspect of this investigation work, the size was kept at fifty which is again computed based on sample size convention on determination, the table for sample size by Krejcie and Morgan, (1970), suggests a specific size from a definite population that is deemed to provide a representative data of a characteristic of that particular population that could be generalizable within the field of survey type research. The population targeted were personnel involved in compliance, audit and IT security from a number of selected banks. This sample size can be concluded as sufficient.

With regards to the qualitative aspect of the study the sample size of 10 participants was determined by the approach to sampling called information power (Malterud, Siersma & Guassora, 2016). The rationale for the small sample is that if participant participants possess great expertise, the research question is narrow, and quality of the conversation is high then a smaller sample is adequate. This was further supported by the principle of data saturation, as the researcher observed that interviews yielded increasingly similar responses and few new themes emerged after the

eighth interview, suggesting that 10 interviews were adequate to capture the range of participant perspectives.

Sampling techniques

Sampling is the technique of selecting some people from a larger population to gather data representative of the larger population and relevant to the research goal (Kumar, 2019). In this study, the major non-probability sampling techniques used were purposive sampling and snowball sampling.

Purposive Sampling

Purposive sampling is a non-probability sampling method in which the researcher intentionally chooses the participants whose characteristics or criteria are directly relevant with the research purpose (Kumar, 2019). A purposive sampling approach was adopted for selecting compliance officers, internal auditors, and financial crime prevention IT security managers with direct operating experience of financial crime prevention technologies from CBZ Holdings and FBC Holdings. This method was deemed most suitable for this research as the research questions would need knowledgeable, experienced answers from people who had the specialised knowledge of AML systems and financial crime detection processes. By choosing participants who have professional expertise in the field, the information gathered was relevant and credible, and the respondents were able to assist in providing substantive information about the nature, effectiveness and difficulty of technology application in their institutions.

Snowball Sampling

Snowball sampling is a non-probability sampling where participants who are initially selected and then asked by the researcher to recommend others who would qualify for the study and can be sampled (Kumar, 2019). To gain further insights into the compliance and IT security field where some participants were not readily available to the researcher due to the sensitive and restricted nature of the financial crime prevention environment, snowball sampling technique was applied as a complementary sampling method to purposive sampling. This was a suitable method for this study as the financial institutions were located in a very confidential and security sensitive environment, and it was hard to have direct access to all the participants involved in the study. An initial group of respondents was therefore selected and their referrals resulted in an additional

group of respondents that had the necessary knowledge and experience and a pathway that respected the institutional access constraints found in financial institutions.

3.6 Research Instruments

The instruments for data collection, which include questionnaires, semi-structured interviews. The use of these instruments was due to their complementary nature in relation to the research methodology adopted in the study.

3.6.1 Questionnaire

The questionnaire is a structured instrument used for data collection, consisting of a series of questions that are predetermined to collect standardised responses from the selected group of participants (Kumar, 2019). The main quantitative instruments used for collecting standardized responses from the selected participants were the questionnaire. Taherdoost (2021) mentions that questionnaires are helpful in collecting standardised data from various respondents quickly. The questionnaire was structured into a few parts: biographical information, technology use, technology effectiveness, operational problems, training and acceptance of the technology, institutional coordination, and recommendations. A 5-point Likert scale was used ranging from Strongly Disagree to Strongly Agree. Not Applicable was also added as an extra option to questions that would not apply to everyone. The N/A responses were not included in the mean calculation.

This questionnaire had several advantages that made it useful to this study. It allowed for the collection of standardised data from a large sample of individuals across two institutions in an efficient and cost-effective way, and helped to facilitate honest responses on the sensitive subject of financial crime prevention (Taherdoost, 2021). It was particularly helpful in the identification of technologies in use, the assessment of perceived effectiveness of the technologies, and the measurement of the operational challenges facing their optimal use, which were the first, second and third objectives of the study. The main drawback of a questionnaire as a tool is that it lacks depth and context in the respondents' answers; closed-ended questions give some answers and may fail to pick up important institutional dynamics (Kumar, 2019). To overcome this challenge, the researcher used a mixed methods approach, using the questionnaire in conjunction with a semi-structured interview guide to allow the researcher to go beyond quantitative responses, further

explore the emerging themes and triangulate between the findings, thereby enhancing the validity and credibility of the study (Creswell & Creswell, 2023).

3.6.2 Semi-structured Interview Guide

The semi-structured interview is a qualitative data collection method that allows the researcher to ask specific questions that are open-ended and flexible, but also allows for the researcher to delve into the answers or delve further into emerging issues during the interview (Kallio et al., 2016). The interviews were conducted using a semi-structured method and were purposively selected involving five senior staff from each institution who had experience and involvement in the financial crime prevention operations. The interviews addressed questions on financial crime detection and prevention, the security versus convenience of the customer, technologies being used, training of employees, and investigations. The interviews were conducted for 45–60 minutes each, were audio recorded with informed consent from the interviewees, and then transcribed for thematic analysis. This procedure ensured the accuracy of the data and minimised the possibility of missing or misreporting the respondents' answers (Kallio et al., 2016).

The semi-structured interview guide was also of significance in this study as it allowed the researcher to delve deeper into the issues raised by the questionnaire and to obtain richer information about institutional experiences and contextual explanations of the experiences that could not be gathered from the quantitative data alone. The interviews were especially relevant to the second and third study objectives in providing detailed accounts of the use of financial crime prevention technologies and the operational challenges faced including the occurrence of false positives, alert fatigue, skills shortage, and coordination issues. The qualitative data was also employed to further analyse, compare, and validate patterns emerging from the quantitative data gathered from the questionnaire, which strengthened the results of the study and its credibility and trustworthiness (Creswell & Creswell, 2023).

3.7 Pilot Testing

A pilot test was done prior to the actual data collection exercise to ensure clarity and understandability of the questions. The pilot sample comprised five respondents from a

commercial bank that was not included in the main study (a Tier 2 bank in Harare). This number was deemed adequate to identify any ambiguities and formatting issues without exhausting potential participants for the main study.

The pilot exercise helped to improve the research instruments in several ways. First, several items on the questionnaire were examined to reduce redundancy and improve clarity. Second, selected interview questions relating to regulatory coordination were revised to improve participant understanding. Thirdly, the structure of the questionnaires was re-arranged for a more logically developed structure including placing the biographical information in the first section of the questionnaire. Therefore, pilot testing allowed for amendments to the structure of research instruments, their wording and overall design. Piloting is considered very important in survey research, as the researcher will be in a position to identify weaknesses in the research instruments before actual study is undertaken. According to Kumar (2019), piloting of the instruments helps the researcher in identifying any vague items in research instrument, thereby improving their clarity and appropriateness. In the present case the sample chosen for pilot test was not considered part of the main study sample and the instruments that had been amended in the pilot testing stage were used for the entire main data collection.

3.8 Validity and Reliability

Several methods were applied to enhance the validity and reliability of the instruments. Firstly, triangulation was applied by collecting data using questionnaires and semi-structured interviews. The researcher was allowed to compare results obtained from two different sources, thereby strengthening the consistency of the findings. Secondly, content validity was maximized by designing the questionnaires and the interview guide directly based on the objectives of the research and literature relevant to technology adoption and financial crime prevention. Face validity of the questionnaire was enhanced as items in the questionnaire were reviewed by research supervisor.

The questionnaire showed consistency through pilot test before main data collection. In pilot test the ambiguity in questions was identified and the instruments were appropriately revised to make them unambiguous, thus achieving internal consistency. Reliability, according to Kumar (2019), is the extent to which research findings are consistent and dependable. Despite the use of Likert type scales in questionnaires and presentation of mean scores of responses in chapter 4, Cronbach

Alpha was not calculated. This was due to the fact that aggregate level data were analyzed, and the respondent level item level data was not saved in the format enabling Cronbach's alpha test. The significance of internal consistency was however addressed through the consistency obtained during the pilot testing, and through designing the questionnaire items from a well-established literature base as well as through triangulation.

3.9 Data Collection Procedure

The data collection process occurred in three distinct stages.

Firstly, the approval was obtained from the institutional and was gained from relevant authorities. Due to the nature of research (employees from sensitive financial environments), permission was required from the institutions at which the data was collected. Creswell and Creswell (2023) emphasise that ethical approval and institutional access are important components of responsible research practice.

Second, questionnaires were distributed to the selected respondents. Participants were given five working days to complete and return the questionnaires. This period was considered sufficient because the questionnaire was concise and focused on issues directly related to the study objectives.

The third methodological approach involved conducting semi-structured interviews with a small sample of those participants selected. A suitable amount of time to have a thorough conversation (between 45 minutes to 1 hour) was factored into each meeting time to accommodate the depth of discussion required. With participants' informed consent, the interviews were audio-recorded and later transcribed for analysis. Audio recording helped ensure accuracy in capturing participants' responses and reduced the risk of omitting important information during note-taking. Kallio et al. (2016) note that recording and transcription improve the accuracy and credibility of qualitative interview data.

3.10 Data Analysis Techniques

The quantitative data gathered from the questionnaires was analysed descriptively, with the use of frequencies, percentages and mean. If Likert scale items had a 'Not Applicable' response, N/A was considered a missing response and was not included in the mean, frequency or percentage analysis for that particular item. This method ensured that only valid answers were used to get descriptive

statistics. Descriptive statistics can be used to summarise and describe the basic characteristics of data collected (Flick, 2020). Such questions were useful because the purpose of the study was to summarize the opinions of the respondents, and to determine common trends, rather than to test hypotheses with statistical tests. The findings were displayed in tabular form and in bar chart for easy understanding.

Clarke (2021) defined thematic analysis as the process of discovering, structuring and comprehending patterns of meaning in the qualitative data. The study adopted a six steps approach of thematic analysis which includes familiarisation with data, coding, theme generation, theme review, theme definition and report writing. This was the suitable method for this research because it enabled the researcher to systematically understand the views of the participants.

3.11 Ethical Considerations

The research followed the key ethical standards expected in academic studies. Informed consent was obtained from each participant prior to their involvement in the research. The aim of the research, its voluntary nature, and the possibility to leave the project at any time without facing consequences were explained to participants. Ethical approval and permission from institutions were secured prior to the start of data collection, as suggested by academic research tradition (Creswell & Creswell, 2023; Kumar, 2019).

Names were not written on the questionnaires, and coding was applied instead to safeguard anonymity. The collected data were kept securely on a password-protected computer and were used only for academic purposes. These measures were crucial because the study involved employees from regulated financial institutions where confidentiality is of great importance (Creswell & Creswell, 2023; Flick, 2020; Kumar, 2019).

3.12 Limitations of the Study

The study was confined to CBZ Holdings and FBC Holdings, which limits the applicability of the findings across the banking sector in Zimbabwe. Access to some confidential institutional information was restricted because the subject involved sensitive issues of financial crime prevention. In addition, the sensitivity of the topic may have made some participants cautious in their responses. Time constraints also affected the depth of research processes.

Cronbach's Alpha was not computed because the dataset used for analysis consisted of aggregated responses, and respondent-level item data were not retained in a format suitable for internal consistency testing. This limitation is acknowledged in the interpretation of the findings. These factors should be considered when interpreting the findings, although they do not reduce the value of the study.

3.12 Chapter Summary

The methodology adopted in the investigation of the role played by technology in detecting and preventing financial crime in the Zimbabwean banking industry, specifically at CBZ Holdings and FBC Holdings, was highlighted in this chapter. Pragmatism was the research philosophy adopted to justify the integration of quantitative and qualitative approaches. The methodology which served as the framework of this study is a convergent parallel mixed method case study research approach. This chapter is a detailed presentation on identification of target population, deciding the sample size and selection of the research respondents, development and adaptation of the research instrument, administration of the pilot study, pilot tested the reliability and validity of the measuring devices, protocol followed during data collection, data analysis procedures, ethical considerations, and limitations of the methodological design. The next chapter presents the data analysis that will be followed to present the findings from the collected evidence.

CHAPTER FOUR

DATA ANALYSIS, INTERPRETATION AND PRESENTATIONS

4.1 Introduction

This chapter brings together the results of the questionnaires that were completed and semi-structured interviews that were undertaken with employees of CBZ Holdings and FBC Holdings, as well as the findings from the aforementioned organisations. The results are presented and analysed in order to correspond to the central purpose of the study, as well as its specific research objectives, which all were aimed at the investigation of the role of technology in preventing financial crime in Zimbabwe's banking industry. Quantitative findings are presented in tabular format, whilst the qualitative findings are evaluated with reference to themes using the method of theme analysis and the illustrative findings were derived by quoting the interviews word for word.

4.2 Response Rate

Table 3: Questionnaire Response Rate

Bank	Distributed	Returned	Valid	Response Rate (%)
CBZ Holdings	25	22	20	80
FBC Holdings	25	21	20	80
Total	50	43	40	80

Source: Field Survey (2026) (N=50)

As shown in Table 3, 50 questionnaires were distributed 25 per bank. Of these, 43 were returned, 40 of which were valid for analysis, yielding an overall valid response rate of 80 %. CBZ Holdings and FBC Holdings each contributed 20 valid responses. The remaining three returned questionnaires were deemed invalid due to incomplete data, specifically the omission of multiple questions. In the study, an 80 per cent response rate was achieved which was sufficient for statistical analysis and the risks from bias in responses were minimized as a result of the number of people participating in the study.

Table 4: Interview Completion Rate

Bank	Targeted	Conducted	Response Rate (%)
CBZ Holdings	5	5	100
FBC Holdings	5	5	100
Total	10	10	100

Source: Field Interviews (2026) (N=10)

Table 4 indicates that 10 semi-structured interviews were conducted in addition to the questionnaires. All scheduled interviews (5 from each bank) were successfully completed, representing a 100 % completion rate. This means a large number of interviewees were available and prepared to share their time perhaps due to the pre-arranged interview time, meaning a total of 50 questionnaires and 10 semi-structured interviews done.

4.3 Demographic Profile of Respondents

Table 5: Demographic Characteristics of Respondents

Variable	Category	CBZ Holdings	FBC Holdings	Total	%
Gender	Male	11	10	21	52.5
	Female	9	10	19	47.5
Age	18-30	3	4	7	17.5
	31-40	9	8	17	42.5
	41-50	6	6	12	30.0
	51+	2	2	4	10.0
Qualification	O Level	1	1	2	5.0
	A Level	2	3	5	12.5
	Diploma	6	5	11	27.5
	Degree	8	8	16	40.0

	Postgraduate	3	3	6	15.0
Position	Manager	5	5	10	25.0
	Officer	7	8	15	37.5
	Clerk	3	2	5	12.5
	Compliance Officer	5	5	10	25.0
Years of service	Under 1	2	3	5	12.5
	2-5	8	7	15	37.5
	6-10	6	6	12	30.0
	11+	4	4	8	20.0

Source: Field Survey (2026) (N=40)

The demographics analysis revealed that the research managed to collect the opinions from employees that are directly in touch with operational activities. A majority of the respondents were aged 31-40, this indicates that those individuals are at the peak of their careers and are sufficiently familiar with the banking systems. The qualifications of the respondents were sound, with degree holders forming the majority. It appears that the respondents were sufficiently informed to make educated opinions on financial crime prevention technologies.

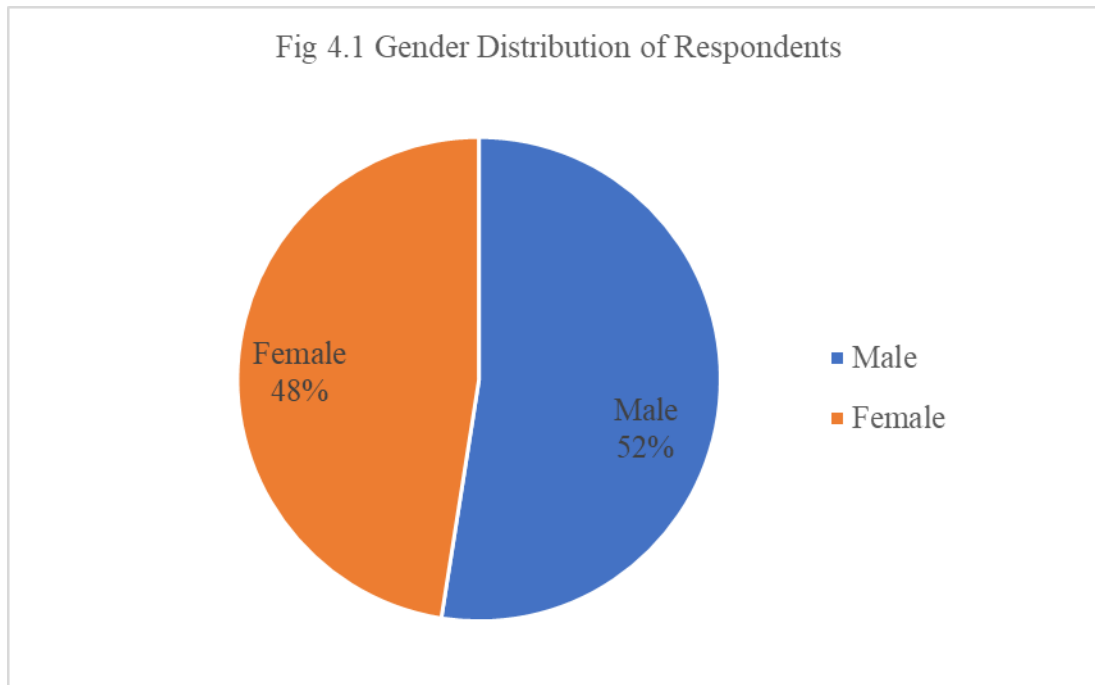


Figure 2: Gender distribution

Figure 2 also reiterates how split the sample was between male and female. With 52.5% of the sample being male and 47.5% of the sample being female, there was no large over- or under-representation of either gender.

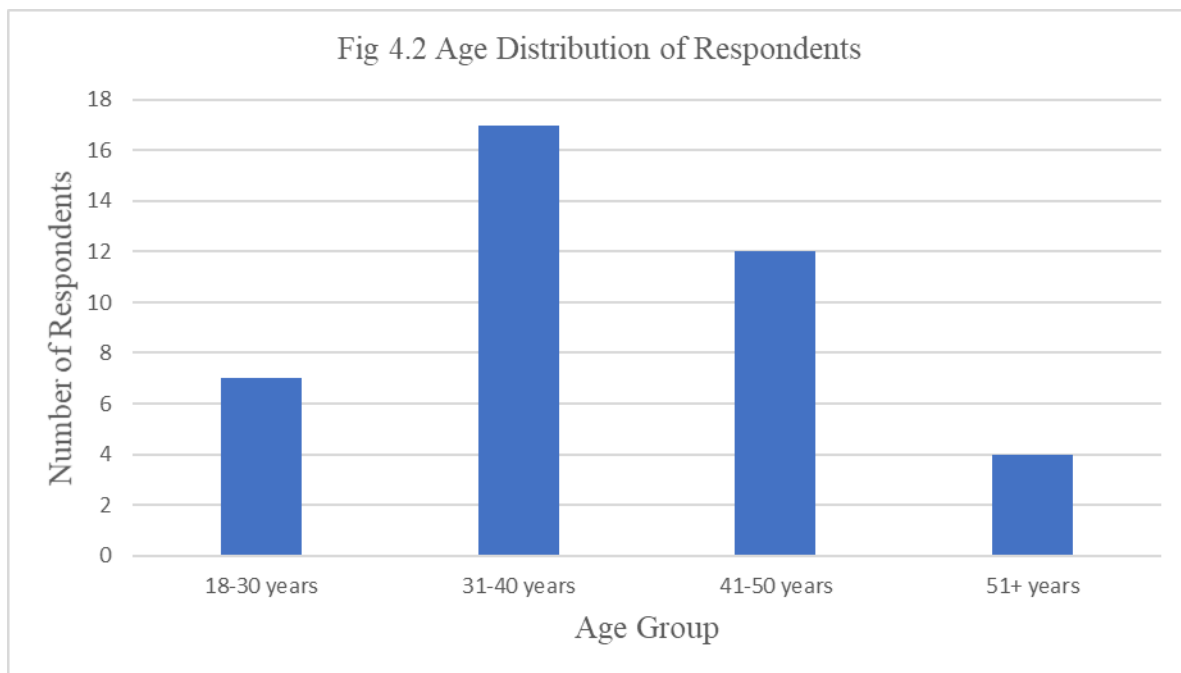


Figure 3: Age distribution

Figure 3 shows the age distribution corresponding to Table 4. It is observed that most respondents were concentrated in the 31–40 and 41–50 age groups, which supports the relevance of their responses.

4.4 Research Findings and Discussion

This section presents an overview of the key findings of the study in relation to the four research objectives. The findings are derived from both the questionnaire and semi-structured interviews and are interpreted in light of the Diffusion of Innovations Theory (Rogers, 1995) and the Technology Acceptance Model (Davis, 1989).

Objective 1: To identify the financial crime prevention technologies currently used by commercial banks in Zimbabwe

The results suggest that there is a strong reliance on traditional, first-generation compliance systems in both institutions, and a striking lack of more advanced technological systems. The Diffusion of Innovations Theory (Rogers, 1995) explains this pattern by highlighting the factors of perceived complexity, resource intensiveness and limited trialability as the major factors that delay the uptake of innovations in resource constrained environments. These results are in line with Dube and Ndlovu (2023) and Chitimira (2021) who report that rule-based systems are still in use and that Zimbabwe is still lagging behind in the implementation of intelligent AML technology. More detailed results are given in Section 4.5 for this objective.

Objective 2: To assess the effectiveness of these technologies in identifying and reporting suspicious transactions to the Financial Intelligence Unit of Zimbabwe

The results show a fundamental conflict between the formal use of financial crime prevention technologies and their capacity to be effective in creating meaningful outcomes in financial crime prevention. Collectively, high levels of false positives, weaknesses in STR reporting processes and limited perceptions of crime reduction suggest that these technologies are not achieving their full crime prevention potential. Viewed through the lens of the TAM, low perceived usefulness among compliance officers contributes to reduced operational engagement, including alert fatigue and selective investigation. It aligns with the study findings of Arner, Barberis and Buckley (2017)

and Dube and Ndlovu (2023) and Jimu and Chimwai (2025) which show a systemic gap between detection at the bank level and enforcement at the national level. A detailed analysis is given in section 4.6.

Objective 3: To investigate the technical, financial and human capital challenges that impede the optimal use of financial crime prevention technologies in Zimbabwean banks

The findings reveal interconnected financial, institutional and human capital barriers that reinforce one another and hinder the optimal use of financial crime prevention technologies. The cost of technology, the lack of inter-institutional coordination with FIUZ, lack of human resources, technological system interoperability failures, and physical infrastructure restrictions all make technology usage suboptimal. These barriers are associated with the characteristics of complexity, lack of compatibility and low trialability of the new technology, as explained by the Diffusion of Innovations Theory (DIT) of Rogers (1995); training problems and interface complexity affect the perceived ease of use, as described by the Technology Acceptance Model (TAM) of Davis (1989). The results of this study are supported by the results of Dube and Ndlovu (2023), Manhida and Nkomo (2024), Jimu and Chimwai (2025) and Mashizha and Kanengoni (2024). A more detailed analysis of the data is provided in Section 4.7.

Objective 4: To recommend strategies for improving the adoption of emerging technologies in financial crime prevention within Zimbabwean banks

The findings indicate that technology adoption through market mechanisms alone is insufficient to strengthen financial crime prevention in Zimbabwe's banking sector due to existing structural and investment constraints. Policy intervention is thus recommended, specifically by creating enabling frameworks, fiscal policies and capacity building programmes. To help reduce perceived complexity, Rogers (1995) advocates phased implementation and pilot programmes to reduce perceived complexity and encourage adoption, while Davis (1989) suggests continued investment in staff development and improvement of the usability of systems is a necessary pre-condition for successful technology acceptance. The recommendations are in line with those of Chitimira (2021), Dube and Ndlovu (2023) and Jimu and Chimwai (2025), which are discussed in detail in chapter Five.

4.5 Technologies Used for Financial Crime Detection

Table 6: Technology Adoption by Bank

Technology	CBZ Holdings %	FBC Holdings %	Total %
Rule-based systems	95	90	92.5
Two-factor authentication	90	90	90
Data Analytics Tools	75	80	77.5
Biometric authentication	65	70	67.5
AI /Machine Learning	30	45	37.5

Source: Field Survey (2026)

These results show a technology adoption hierarchy. The top two are rule-based systems of 92.5 % and two-factor authentication 90 %, with AI and machine learning only 37.5 %. This is not coincidental. Dube and Ndlovu (2023) explain that rule-based systems continue to be widely used in Zimbabwean banking because they require less sophisticated infrastructure. This reliance, however, has an important drawback: rule-based systems only detect known patterns and are therefore less effective against emerging threats. Risk aversion appears to have outweighed the perceived benefits of innovation, limiting the adoption of AI.

Data analytics tools are moderately common (77.5 %), suggesting a gradual shift toward data-informed detection. Yet, AI/ML adoption remains low, with only 30 % of CBZ Holdings and 45 % of FBC Holdings adopting these technologies. Chitimira (2021) argues that a major reason behind this tendency is the lack of manpower, costs involved and infrastructure. This corresponds to Rogers' Diffusion of Innovations theory that a complex and expensive technology will be slow in adoption. For Zimbabwe, Artificial Intelligence and Machine Learning may still be considered unknown, and risky technologies.

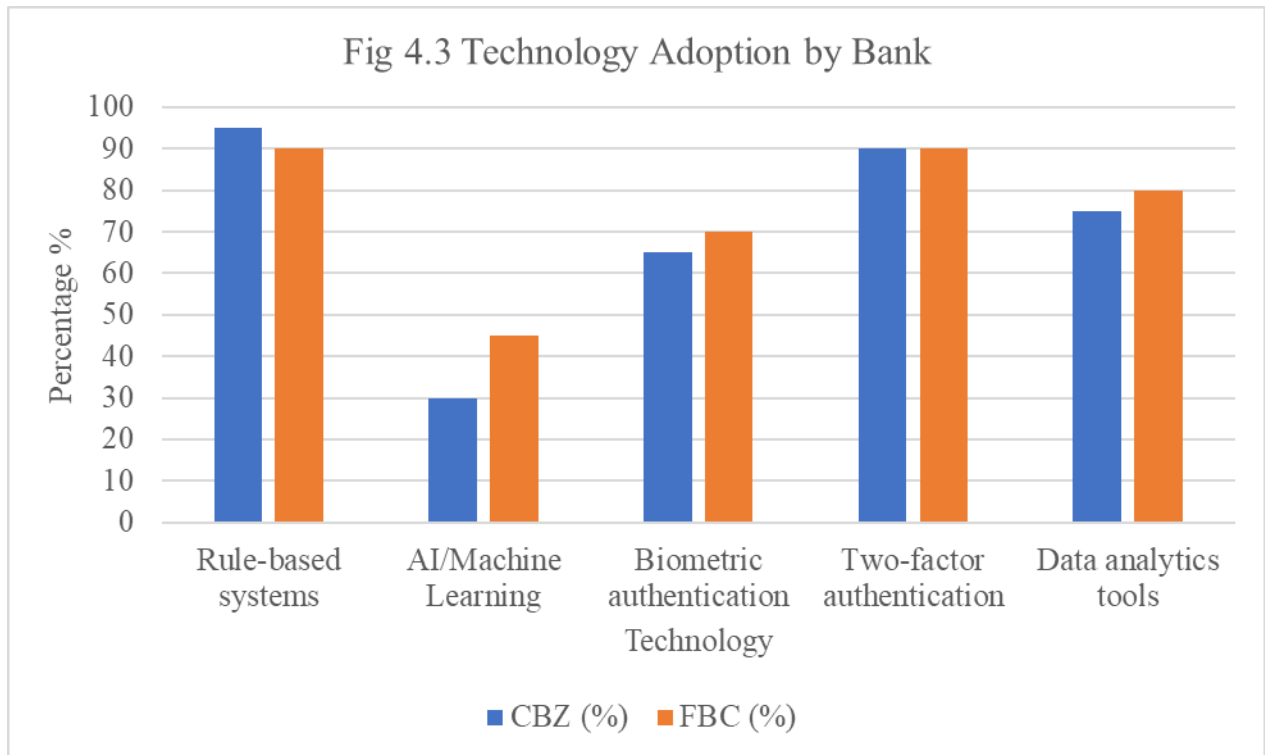


Figure 4: Technology adoption

Figure 4 shows that both CBZ Holdings and FBC Holdings use similar technologies.

Table 7: Perceived Effectiveness (Likert Scale: 1–5)

Statement	CBZ Holdings	FBC Holdings	Overall	Interpretation
Systems accurately detect suspicious transactions	2.95	2.75	2.85	Neutral
Systems generate too many false positive alerts	3.70	3.50	3.60	Agree
STRs are submitted to FIUZ on time	2.75	2.50	2.63	Neutral
Financial crime has reduced since technology was introduced	3.10	2.90	3.00	Neutral

Source: Field Survey (2026)

4.6 Effectiveness of Current Technologies

From the outcomes it can be seen that the participants question the performance of new technologies. The highest agreement occurred when questioned about false positives, which proves that newer systems provide numerous alerts that cannot be linked with suspicions. This point is of significance because with a large number of alarms employees are unable to pay attention to actual threats, as suggested by Arner, Barberis and Buckley (2017) and Dube and Ndlovu (2023) with rules-based systems creating numerous false alarms.

Neutral opinions regarding the discovery of suspicious behaviour as well as the decrease of crime levels after implementing technology reflect that the respondents did not perceive the preventive impact of such tools. Therefore, while technology might play a role in control and monitoring the role it plays in diminishing crime is not evident, which coincides with statements by Ferwerda,

Deleanu and Unger (2021) when they confirm that only by using technology does not automatically assure high performance without correct systems.

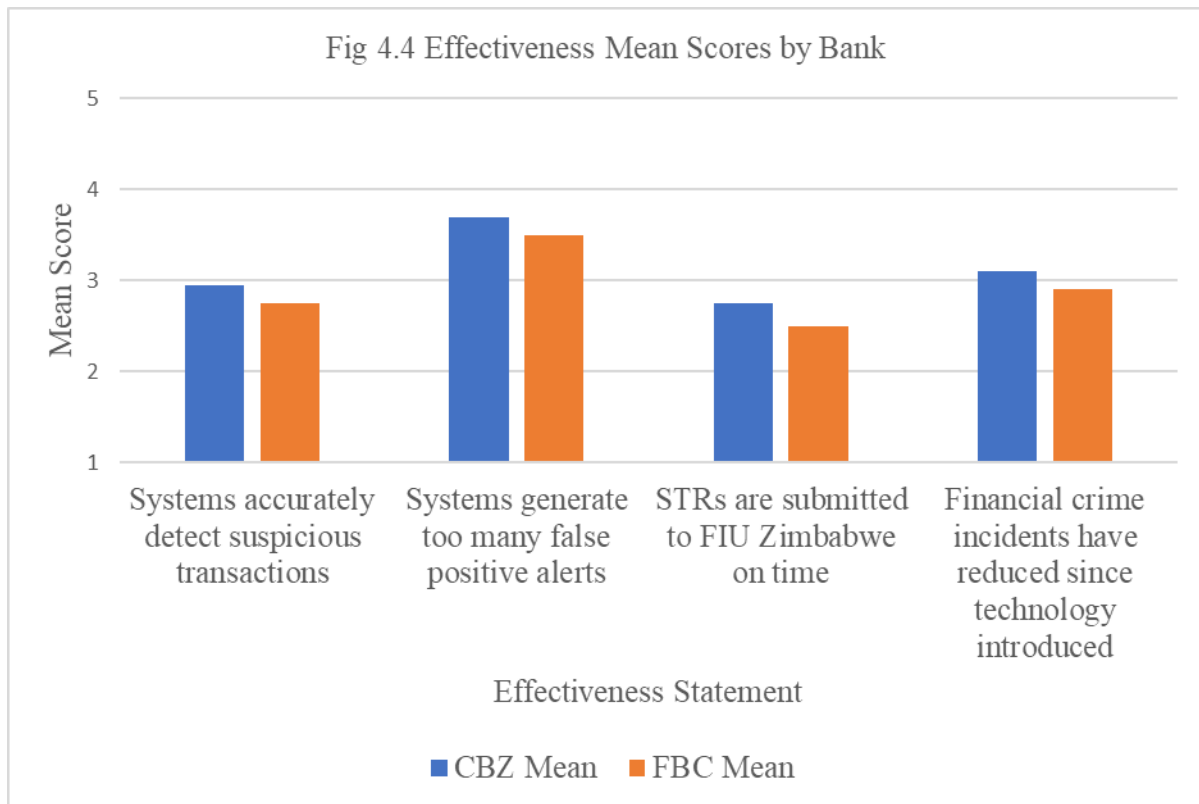


Figure 5: Effectiveness mean score

Figure 5 shows that false positives have the highest score, confirming that this is the most serious operational concern.

4.7 Challenges Affecting Technology Use

Table 8: Operational Challenges (Likert Scale: 1–5)

Challenge	CBZ Holdings	FBC Holdings	Overall	Interpretation
-----------	--------------	--------------	---------	----------------

High implementation cost	3.70	3.50	3.60	Agree
Weak FIU coordination	3.65	3.25	3.45	Agree
Lack of skilled	3.60	3.25	3.43	Agree
System integration issues	3.40	3.10	3.25	Neutral
Poor infrastructure	3.20	2.95	3.08	Neutral

Source: Field Survey (2026)

High cost of implementation was found to be the biggest challenge. This is suggesting that even though banks see benefits in these high-tech technologies, they are restricted by the amount of financial resources they can commit to acquiring and maintaining such systems and technology upgrades. It can also be noted that cost was considered to be one of the major challenges limiting RegTech adoption in Zimbabwe by Dube and Ndlovu (2023). This assertion also complements Chitimira's (2021) assertion that the prosecution of financial crimes in Zimbabwe is hampered by over-arching institutional and economic constraints.

Poor coordination with the FIUZ was found to be the second biggest challenge in which respondents indicated that external regulatory follow-up was the main limitation. This is critical in that, the ability to effectively prevent financial crimes relies not only on the systems available at the bank but also on how effectively these systems alerts are reviewed and investigated by the FIUZ. This finding is also corroborative to Jimu and Chimwai's (2025) description of FIUZ capacity as a key constraint to the framework for anti-money laundering activities in Zimbabwe.

Lack of skilled staff was equally important in revealing that the biggest weakness in prevention of financial crimes was human capacity. This simply indicates that if the banks fail to have skilled personnel who can identify and properly investigate suspicious alerts, their high-tech systems will remain of limited effectiveness. This can be demonstrated by the fact that limited technical

capacity remains an impediment to fraud detection by Zimbabwean financial institutions according to Manhide and Nkomo (2024).

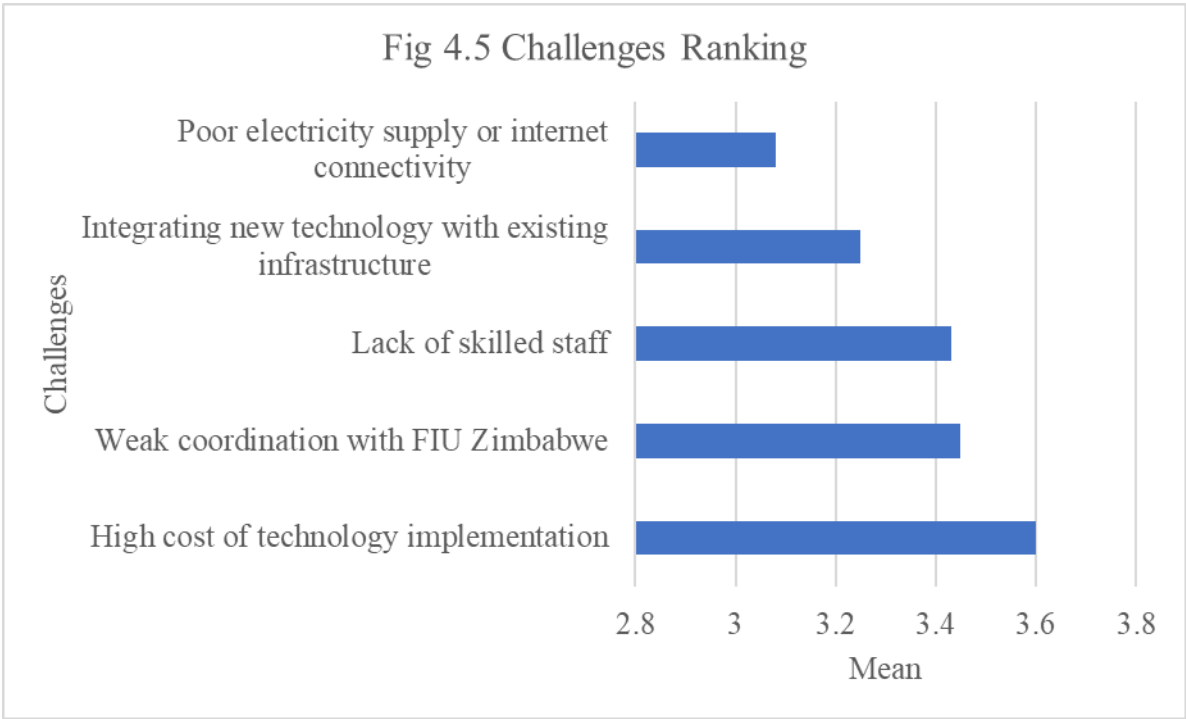


Figure 6: Challenges ranking

Figure 6 shows that high implementation cost is the leading challenge, followed by weak FIU coordination and lack of skilled staff.

4.8 Interview Findings

The interviews produced five key themes:

- High technology costs, reported by 6 out of 10 respondents.
- Weak FIU coordination, reported by 8 out of 10 respondents.
- Lack of skilled staff, reported by 7 out of 10 respondents.
- System integration issues, reported by 5 out of 10 respondents.
- Infrastructure challenges, reported by 4 out of 10 respondents.

The results from the interview reinforce those from the questionnaire and suggest that, to some extent, the barriers to efficient financial crime prevention are both systemic and human as opposed to being solely technological. Insufficient cooperation with FIU was the most commonly raised

concern suggesting that respondents regard financial crime prevention as a systemic phenomenon that cannot be addressed at the banking level alone. The results are in line with the findings of Jimu and Chimwai (2025) who cite insufficient FIU analytic capacity as the main weakness in Zimbabwe's anti-money laundering framework.

The one respondent claimed, "*The cost of upgrading our AML system is very high and management does not sanction huge expenditure where there are no immediate returns*", pointing to the lack of finances to purchase updated AML systems. The study by Dube and Ndlovu (2023) reiterates the cost barrier in adoption of RegTech among banks in Zimbabwe. This finding also aligns with the view of Arner, Barberis and Buckley (2017) who emphasize that while technology costs can decrease as RegTech develops, they remain a barrier to investment for many institutions (#1)

The other participant also said, "*We normally wait for feedback from FIU, but there is delay in inter-institution co-operation*", implying an unsatisfactory relationship between the two institutions and potentially an ineffective suspicious transaction reporting system. This is supported by Jimu and Chimwai (2025) who view poor FIU analytic capability and slow turnaround times of FIU as major weaknesses in anti-money laundering mechanisms in Zimbabwe (#2)

A compliance officer reported: "*We have the systems but not people who know how to use them, although training exists, it is quite basic.*" This shows a lack of sufficiently knowledgeable human capital, which is also supported by Manhide and Nkomo (2024) who regard insufficient technical expertise as one of the continuing reasons why fraud is still rampant in Zimbabwean banks as a result of the sub-optimization of the systems (#3)

The interviewee stated: "*The fraud detection system is not directly integrated with the core banking system; hence we need to manually export and import, leading to delays.*" This demonstrates lack of integration between various systems as reported by 5 out of 10 respondents, and as noted by Arner, Barberis and Buckley (2017) system interoperability is a prerequisite for effective RegTech utilization (#4)

An interviewee lamented: "*There is abundance of alerts from the system, but most of them are not suspicious.*" The same challenge as identified in the quantitative analysis (false positive problem) implies inefficiency as operators waste time monitoring false alarms instead of focusing on actual

suspicious, as seen in the case of Arner, Barberis and Buckley (2017) and Schmar (2021) who consider false positives a common feature of rule-based AML systems (#5)

An interview respondent had this to say, "*The system is often offline due to persistent power outages and poor internet connectivity and sometimes is down for hours.*" This implies infrastructural weaknesses among banks in Zimbabwe. According to Mashizha and Kanengoni (2024), lack of adequate power and internet infrastructure often compromise cyber security activities of banks in Zimbabwe, and therefore, this interviewee's experience is not unique (#6)

4.9 User Training and Acceptance

Table 9: User Training and Acceptance

Statement	CBZ Holdings	FBC Holdings	Overall	Interpretation
Systems useful	2.75	2.50	2.63	Neutral
Easy to use	2.95	2.75	2.85	Neutral
Adequate training	3.25	2.95	3.10	Neutral

Source: Field Survey (2026)

In respect to user training and acceptance, the results of the analysis can be considered neutral since the respondents did not have any strong positive or negative attitude towards the technologies currently being used. Thus, despite the availability of the technologies, their perceived usefulness and easiness remain moderate rather than strong. Davis (1989) proposed the technology acceptance model.

This theory says that two specific factors, i.e. The perceived usefulness of the new technological innovation in improving the performance and perceived ease of use of the new technological innovation influence the attitudes of people to use the new technological innovation, and eventually, attitudes and the intention to use the new technological innovation. The neutral scores for both usefulness (2.63) and ease of use (2.85) suggest that respondents have not yet reached the acceptance threshold predicted by TAM, which may explain the moderate levels of technology utilisation observed in this study.

The neutral attitude towards training is significant in the sense that the implementation of the system is not likely to have been supported by capacity building measures. Practically speaking, inadequate training might result in inefficiency in the operation of such systems despite how good they are designed since the personnel may lack confidence in understanding the output of such systems or using the systems effectively. According to Manhide and Nkomo (2024), the successful use of technologies requires not only having systems in place but also the ability and readiness of people to use such systems. The highest average score for adequate training was 3.10.

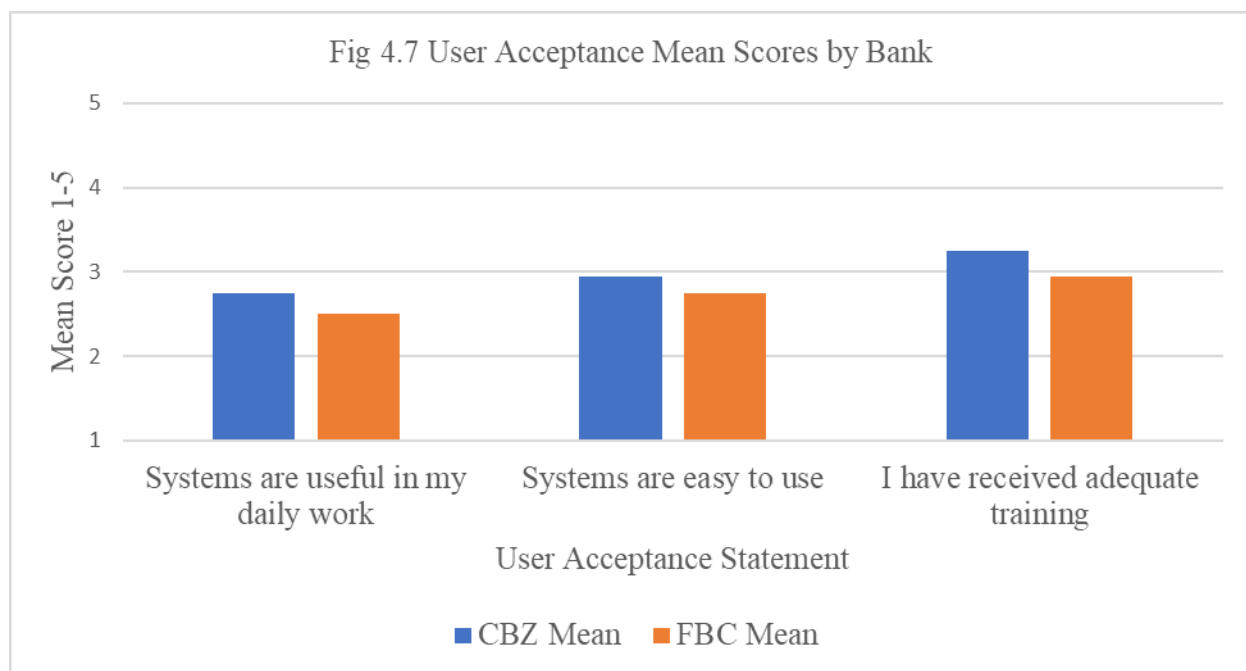


Figure 7: User acceptance statement:

Figure 7 illustrates that the three statements recorded relatively close scores, reinforcing the generally neutral pattern in user perceptions.

4.10 Chapter Summary

It was concluded that even with technology adoption, rules-based systems are the prevailing mode of prevention for financial crime in the banks studied, with Artificial Intelligence and machine learning yet to be widely applied. Furthermore, false positive detection was reported as one of the most difficult obstacles during implementation while high cost of implementing the technology, poor cooperation between banks and FIUZ, and absence of adequate technically competent personnel impeded the effectiveness of current technological tools. User training and technological

acceptance may be considered moderate. It can therefore be hypothesized that despite technology adoption in Zimbabwean banks, their actual use in preventing financial crime do not translate to being fully effective, but subject to various institutional, functional, and human resource barriers. The presence of technology cannot guarantee financial crime prevention success.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The concluding chapter is a synthesis of the empirical data collected during the investigation and distils these into key results that form conclusions and then forward-looking recommendations for an effective framework for technology solutions to prevent financial crime within Zimbabwe's banking sector. This study was geared towards assessing the use and adoption rate of technologies for financial crime prevention, and the sample was CBZ Holdings and FBC Holdings. In addition, the study pointed out the implications for the banking institutions, regulatory coordination and the future research.

5.2 Findings

The study revealed that in Zimbabwean banks there are various technologies used in the fight against financial crime. Rule-based systems were widely adopted (92.5%), followed by two-factor authentication (90%), data analytics tools (77.5%) and biometrics technology (67.5%). The level of the usage of advanced technology like AI and machine learning in fighting against financial crime was found to be relatively low in the surveyed banking institutions (37.5%), and adoption of Artificial intelligence and machine learning in CBZ Holdings (30%) was lower than that in FBC Holdings (45%). The findings implied that banks still rely heavily on traditional rule-based systems rather than on predictive systems.

The technologies used were moderate in their efficiency in detecting and reporting financial crime. One of the significant findings was the excessive false positive alerts that the system generates which could possibly create work fatigue for the staff responsible for checking transactions, average mean was 3.60, and accuracy of the detection of suspicious transactions were 2.85, timeliness of submitting Suspicious Transactions Reports to FIUZ were 2.63, and perception of reduction in financial crimes had average mean of 3.00. This implied that they are only moderately effective to assist in fight against financial crimes. Challenges that hampered efficiency usage of financial crime prevention technology were highest on cost of implementation (mean 3.60) followed by weak coordination with the FIUZ (mean 3.45), Lack of specialized staff (mean 3.43),

Integration problems (mean 3.25) and Infrastructural problems (mean 3.08). Programme of staff development was rated moderately effective with a mean score of 3.10. The technology uptake indicated a mean score of 2.85 for Perceived Ease of use and a mean score of 2.63 for Perceived use. The analytical results provided empirical support for the employee resistance, user attitude, system use and the employee competency collectively stood at the moderate ranges. These findings align with the theoretically derived statement of TAM suggesting user's attitude towards usefulness and usability of technology contribute to its adoption. Through interviews, important themes emerged. Cost of technology, weak coordination with FIUZ, lack of specialised personnel, system integration issues and infrastructure problems are some of the critical issues to address.

5.3 Conclusions

The following conclusions are made in accordance with the research objectives of the study.

Objective 1: To determine the financial crime prevention technologies adopted by commercial banks in Zimbabwe.

The study concludes that CBZ Holdings and FBC Holdings have adopted various financial crime prevention technologies and the most adopted technologies are rule-based systems (92.5%) and two-factor authentication (90%). Data analytics (77.5%) and biometric authentication (67.5%) are also employed and although adopted at relatively lower rates, advanced technologies such as AI and machine learning were also found to be present in the banks studied (37.5%). The result indicates that Zimbabwean banks continue to employ rule-based systems for transaction monitoring rather than artificial intelligence or machine learning techniques to mitigate financial crime.

Objective 2: To evaluate the effectiveness of these technologies in detecting and reporting suspicious transactions to FIUZ.

The findings indicate that the effectiveness of current financial crime prevention technologies employed is moderate. Operational challenges of high number of false positives (Mean=3.60) in transaction monitoring were highest among other challenges. Detection of suspicious transactions (Mean=2.85), timeliness in filing Suspicious Transaction Reports with the FIUZ (Mean=2.63) and reduction in financial crime (Mean=3.00) was rated as moderate to neutral. This means that despite

the monitoring systems having increased monitoring capacity, other factors also need to be in place for the full achievement of the objective.

Objective 3: To identify and examine technical, financial, and human capital challenges that limit the optimum use of financial crime prevention technologies in banks in Zimbabwe.

A number of operational and institutional challenges limit the effective usage of the financial crime prevention technologies. High implementation costs (Mean=3.60) proved to be the highest barrier to the successful adoption and utilisation of financial crime prevention technologies followed by weak coordination with FIUZ (Mean=3.45), inadequate skilled personnel (Mean=3.43), system integration (Mean=3.25) and infrastructure inadequacy (Mean=3.08) moderate level of user training (Mean=3.10) was observed. Technology acceptance level was found to be moderate (usefulness = 2.63, ease of use = 2.85) hence implying the existence of other factors also playing a part to the ineffective use of financial crime prevention technologies apart from technology itself.

Objective 4: To propose strategies that may be adopted for better technology adoption of emerging financial crime prevention technologies.

The study recommends the use of phased investment plans to incorporate AI and ML in their financial crime prevention systems, periodical review of threshold limits for monitoring systems to curb the problem of false positives, dedicated budget for acquiring and maintaining financial crime prevention technologies, establishment of reporting protocols with timelines between banks and FIUZ to strengthen coordination and provision of structured and comprehensive training for staff who are manning the systems.

Overall Conclusion:

Technology is of essence in financial crime prevention but insufficient alone, without proper support of institutional cooperation, skilled personnel, sufficient funds, and continuous training. Thus, for better financial crime prevention mechanisms in banks in Zimbabwe both technology and organisational support are crucial.

5.4 Contribution to Knowledge

This study makes an empirical contribution to the existing body of knowledge on financial crime prevention technology within the banking sector in Zimbabwe. Although previous studies have

focused on adoption of anti-money laundering technologies within banks globally, this study examined both the types of technology used and their effectiveness as perceived by users within the Zimbabwean banking sector.

Theoretically, this study extends previous application of the Diffusion of Innovations Theory and Technology Acceptance Model within the Zimbabwean context by demonstrating the significance of institutional coordination and economic context in influencing technology adoption and usage effectiveness.

Practically, the findings add value to banks and policy makers by informing them about the challenges that must be overcome to achieve optimum usage and benefits of the technology employed in preventing financial crimes, among these are high implementation costs, poor coordination with FIUZ, lack of skilled personnel, systems integration problems, moderate levels of training and user acceptance.

5.5 Limitations of the Study

Despite achieving its objectives, the study was subjected to certain limitations. Firstly, the study targeted only two banking institutions, CBZ Holdings and FBC Holdings and thus, its findings might not represent the entire banking sector in Zimbabwe, which could also include building societies and smaller banks.

Secondly, reliance is placed on individual opinions rather than an evaluation of actual effectiveness using institutional performance data or criminal statistics as an objective measure of the extent to which each technology prevented crime. The perception of respondents could be influenced by individual experiences, organisational norms, or recollections of past crime incidence.

Thirdly, it was not possible to calculate Cronbach's Alpha as the raw data for Likert scales was not archived post aggregation, reliability was established through pilot study, content validity, face validity and triangulation.

Fourth, the cross-sectional study design captures results at a single point in time; thus it does not indicate any changes in technology adoption trends over time, nor crime trends.

Finally, certain classified and sensitive financial crime prevention information was unobtainable, thus the depth of investigation may be limited by lack of some information.

It is recommended that these limitations be considered in interpreting the results of the study.

5.6 Recommendations

5.6.1 Recommendations for Practice

CBZ Holdings and FBC Holdings

The study recommends that both CBZ Holdings and FBC Holdings gradually and systematically integrate AI and machine learning into their financial crime prevention systems. These systems detect financial crime more effectively than rule-based systems which tend to generate more false positives and are less equipped to handle complex patterns of financial crime. Both institutions should regularly review alert thresholds and configurations in order to identify more genuine risks rather than being overwhelmed by a large number of false positives by the system. Management in both banks should prioritise investment in procurement, maintenance and upgrades of systems used to monitor financial crime, the lack of which emerged as the main challenge impeding the uptake of technology. Both banks should implement structured training programs for staff involved in monitoring financial crime to enhance system confidence, technical ability and proper system utilization.

CBZ Holdings, FBC Holdings and the Financial Intelligence Unit of Zimbabwe (FIUZ)

The study recommends the establishment of reporting protocols between CBZ Holdings, FBC Holdings and FIUZ with clear timelines for review and investigation of STRs to ensure seamless coordination among these institutions and provide a robust mechanism to track investigations and prosecute offenders, an issue identified in interviews with stakeholders.

5.6.2 Recommendations for Future Research

Further research is recommended that covers a wider range of banking institutions in Zimbabwe; small banks, building societies, and others to determine if findings apply across the board. An investigation into the feasibility and costs of using AI and ML technologies in resource constrained institutions is recommended with appropriate cost-benefit analysis. Future research should investigate the nexus between technology effectiveness at the banking level and analytical capacity at the FIU level as well as the process by which a STR eventually results in a successful

investigation and prosecution. Due to the inherent cross-sectional nature of the design of the current research a longitudinal study would prove extremely beneficial in examining the progress of system efficiency in relation to how banking firms continue to implement higher levels of technological advancement. Finally future research could seek to supplement the self-reported perception of the participants by using objective data such as system performance data, as well as real administrative crime statistics to further enhance the credibility of results.

REFERENCES

- Arner, D. W., Barberis, J. and Buckley, R. P. (2017) 'FinTech, RegTech and the reconceptualization of financial regulation', *Northwestern Journal of International Law and Business*, 37(3), pp. 371-413.
- Arner, D. W., Barberis, J. and Buckley, R. P. (2019) 'The evolution of FinTech: A new post-crisis paradigm?', *Georgetown Journal of International Law*, 47(4), pp. 1271-1319.
- Bowen, G. A. (2009) 'Document analysis as a qualitative research method', *Qualitative Research Journal*, 9(2), pp. 27-40.
- Braun, V. and Clarke, V. (2021) *Thematic analysis: A practical guide*. London: SAGE Publications.
- CBZ Holdings Limited (2023) *Integrated annual report 2023*. Harare: CBZ Holdings.
- Chitimira, H. (2021) 'Towards ingenious technology and robust enforcement of financial market laws to curb financial crimes in Zimbabwe', *Potchefstroom Electronic Law Journal*, 24, pp. 1-28.
- Clarke, V. (2021) *Thematic analysis: A practical guide*. London: SAGE Publications.
- Creswell, J. W. (2014) *Research design: Qualitative, quantitative, and mixed methods approaches*. 4th edn. Thousand Oaks, CA: SAGE Publications.
- Creswell, J. W. and Creswell, J. D. (2023) *Research design: Qualitative, quantitative, and mixed methods approaches*. 6th edn. Thousand Oaks, CA: SAGE Publications.
- Creswell, J. W. and Poth, C. N. (2018) *Qualitative inquiry and research design: Choosing among five approaches*. 4th edn. Thousand Oaks, CA: SAGE Publications.
- Davis, F. D. (1989) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', *MIS Quarterly*, 13(3), pp. 319-340.
- Dube, L. and Ndlovu, S. (2023) 'The RegTech dilemma: Adoption challenges in Zimbabwe's Tier 1 banks', *African Journal of Business Management*, 17(2), pp. 55-67.
- Eastern and Southern Africa Anti-Money Laundering Group (2023) *Mutual evaluation report: Zimbabwe*. Dar es Salaam: ESAAMLG.
- FBC Holdings Limited (2023) *Annual report 2023*. Harare: FBC Holdings.
- Ferwerda, J., Deleanu, I. and Unger, B. (2021) 'Corruption and money laundering: A complex relationship', *European Journal of Law and Economics*, 51(2), pp. 215-238.
- Financial Action Task Force (2021) *International standards on combating money laundering and the financing of terrorism and proliferation*. Paris: FATF/OECD.

Financial Action Task Force (2022) *Guidance on digital identity for financial integrity*. Paris: FATF.

Financial Intelligence Unit of Zimbabwe (2022) *Annual report 2022*. Harare: Reserve Bank of Zimbabwe.

Financial Intelligence Unit of Zimbabwe (2023) *Annual report 2023*. Harare: Reserve Bank of Zimbabwe.

Flick, U. (2020) *An introduction to qualitative research*. 7th edn. London: SAGE Publications.

Gutsa, E. (2024) *The role of technology in detecting and preventing fraudulent activities of a financial institution focusing on CBZ Limited Bank Zimbabwe*. Undergraduate dissertation. Bindura University of Science Education.

Institute for Security Studies (2023) *African organised crime index: Zimbabwe country report*. Pretoria: ISS.

Jimu, T. and Chimwai, L. (2025) 'The role of financial intelligence units in Zimbabwe: Combating money laundering using FATF recommendations', *Kuveza neKuumba Journal of Design, Innovative Thinking and Practice*, 4(1-2), pp. 187-248.

Kallio, H., Pietilä, A.-M., Johnson, M. and Kangasniemi, M. (2016) 'Systematic methodological review: developing a framework for a qualitative semi-structured interview guide', *Journal of Advanced Nursing*, 72(12), pp. 2954-2965.

Krejcie, R. V. and Morgan, D. W. (1970) 'Determining sample size for research activities', *Educational and Psychological Measurement*, 30(3), pp. 607-610.

Kumar, R. (2019) *Research methodology: A step-by-step guide for beginners*. 5th edn. London: SAGE Publications.

Malterud, K., Siersma, V. D. and Guassora, A. D. (2016) 'Sample size in qualitative interview studies: Guided by information power', *Qualitative Health Research*, 26(13), pp. 1753-1760.

Manhide, T. and Nkomo, D. (2024) 'Determinants influencing the upsurge of electronic banking frauds in Zimbabwe', *Journal of Research and Innovation for Sustainable Society*, 6(1), pp. 45-62.

Mashizha, M. and Kanengoni, P. (2024) 'The adequacy of cybersecurity in financial institutions in Zimbabwe', *International Research Journal of Business Studies*, 17(3), pp. 317-331.

Morgan, D. L. (2014) 'Pragmatism as a paradigm for social research', *Qualitative Inquiry*, 20(8), pp. 1045-1053.

Nunnally, J. C. (1978) *Psychometric theory*. 2nd edn. New York: McGraw-Hill.

Reserve Bank of Zimbabwe (2020) *National Financial Inclusion Strategy II (2020-2024)*. Harare: Reserve Bank of Zimbabwe.

Reserve Bank of Zimbabwe (2021) *Bank supervision annual report 2021*. Harare: Reserve Bank of Zimbabwe.

Reserve Bank of Zimbabwe (2023) *Annual report 2023*. Harare: Reserve Bank of Zimbabwe.

Rogers, E. M. (1995) *Diffusion of innovations*. 4th edn. New York: Free Press.

SARPPCO (2022) *Annual report of the Southern African Regional Police Chiefs Cooperation Organisation*. Harare: SARPPCO.

Saunders, M., Lewis, P. and Thornhill, A. (2019) *Research methods for business students*. 8th edn. Harlow: Pearson Education.

Schmar, P. (2021) *Fraud costs: An analysis of global financial crime losses*. London: Financial Crime Research Institute.

South African Banking Risk Information Centre (2024) *Annual crime statistics report 2023*. Johannesburg: SABRIC.

Tachiona, T. M. (2020) *An analysis into the effects of cybercrime on the financial services sector and national development in Zimbabwe*. Master's dissertation. University of Zimbabwe.

Taherdoost, H. (2018) 'A review of technology acceptance and adoption models and theories', *Procedia Manufacturing*, 22, pp. 960-967.

Taherdoost, H. (2021) 'Data collection methods and tools for research; a step-by-step guide to choose data collection technique for academic and business research projects', *International Journal of Academic Research in Management*, 10(1), pp. 10-38.

United Nations Office on Drugs and Crime (2022) *Financial crime and digital transformation: Global threats and responses*. Vienna: UNODC.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) 'User acceptance of information technology: Toward a unified view', *MIS Quarterly*, 27(3), pp. 425-478.

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

Zimbabwe (2013) *Money Laundering and Proceeds of Crime Act [Chapter 9:24]*. Harare: Government of Zimbabwe.

Zimbabwe (2021) *Cyber and Data Protection Act [Chapter 12:07]*. Harare: Government of Zimbabwe.

Zimbabwe Republic Police (2024) *Annual crime statistics report 2023*. Harare: Zimbabwe Republic Police.

APPENDIX 1



BINDURA UNIVERSITY OF SCIENCE EDUCATION

Private Bag 1020
BINDURA, Zimbabwe
Tel: 0271 – 7531-6, 7615
Fax: 263 –271 – 7534

INTELLIGENCE AND SECURITY STUDIES DEPARTMENT

22 May 2026

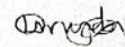
CBZ Holdings and FBC Holdings

RE: REQUEST FOR DATA COLLECTION

Please may you assist our student Gombe Gennah (B222358B) to carry her research in your organization on her topic on “The role of Technology in Financial Crime Prevention. A case study of Zimbabwe’s Banking Sector with reference to CBZ Holdings and FBC Holdings.” She is our final year student at Bindura University of Science Education in the Intelligence and Security Studies Department.

Your assistance to our student will be greatly appreciated.

Regards


Ms L Chinyoka
Chairperson



APPENDIX 2

QUESTIONNAIRE

THE ROLE OF TECHNOLOGY IN FINANCIAL CRIME PREVENTION:

A CASE STUDY OF CBZ HOLDINGS AND FBC HOLDINGS

Dear Respondent

I am a final-year Financial Intelligence student at Bindura University conducting research on the role of technology in financial crime prevention within Zimbabwe's banking sector, with specific reference to CBZ Holdings and FBC Holdings. Your participation is voluntary and all responses will be treated with strict confidentiality for academic purposes only. Please do not write your name on this questionnaire.

Consent: By completing this questionnaire, you voluntarily agree to participate in this study.

Instructions: Please tick [✓] the option that best represents your answer.

SECTION A: BIOGRAPHICAL INFORMATION

Name of Bank

1. Gender

☐ Male ☐ Female

2. Age group

☐ 18–30 years ☐ 31–40 years ☐ 41–50 years ☐ 51+ years

3. Highest qualification

☐ O Level ☐ A Level ☐ Diploma ☐ Degree ☐ Postgraduate ☐ Other

4. Current position

☐ Manager ☐ Officer ☐ Clerk ☐ Compliance Officer ☐ Other

6. Years of service at current bank

☐ Under 1 year ☐ 2–5 years ☐ 6–10 years ☐ 11+ years

SECTION B: TECHNOLOGY ADOPTION AND EFFECTIVENESS

The questions in Sections B to D were derived using a five-point Likert scale to measure respondents' positive or negative responses to each statement. The scale is classified as follows:

1 = Strongly Disagree

2 = Disagree

3 = Neutral

4 = Agree

5 = Strongly Agree

N/A = Not Applicable

1. The bank where I work uses rule-based monitoring systems for financial crime detection.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

2. The bank where I work uses artificial intelligence or machine learning for financial crime detection.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

3. The bank where I work uses biometric authentication for customer verification.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

4. The bank where I work uses two-factor authentication for online transactions.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

5. The bank where I work uses data analytics tools to detect suspicious transaction patterns.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

6. Current monitoring systems accurately detect suspicious transactions.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

7. Monitoring systems generate too many false positive alerts.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

8. Suspicious Transaction Reports (STRs) are submitted to the Financial Intelligence Unit (FIU) Zimbabwe on time.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

9. Financial crime incidents have reduced since current technology was introduced.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

SECTION C: OPERATIONAL CHALLENGES AND INSTITUTIONAL COORDINATION

1. High cost of technology implementation is a major challenge.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

2. Lack of skilled staff to operate technology systems is a major challenge.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

3. Poor electricity supply or internet connectivity disrupts detection systems.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

4. Integrating new technology systems with existing infrastructure is challenging.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

5. Weak coordination with FIU Zimbabwe hinders effective reporting.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

6. The bank where I work has effective communication channels with FIU Zimbabwe.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

7. FIU Zimbabwe provides timely feedback on submitted reports.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

8. Improved coordination with FIU Zimbabwe would enhance financial crime prevention.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

SECTION D: USER TRAINING, ACCEPTANCE AND RECOMMENDATIONS

1. Financial crime detection systems are useful in my daily work.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

2. Financial crime detection systems are easy to use.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

3. I have received adequate training to use financial crime detection systems.

☐1 ☐2 ☐3 ☐4 ☐5 ☐N/A

4. What one improvement would most enhance financial crime detection in your bank?

.....

.....

.....

5. How can coordination between your bank and FIU Zimbabwe be improved?

.....

.....

.....

6. What specific challenges have you experienced when using financial crime detection systems?

.....

.....

.....

THANK YOU FOR YOUR VALUABLE PARTICIPATION

APPENDIX 3

SEMI-STRUCTURED INTERVIEW GUIDE

THE ROLE OF TECHNOLOGY IN FINANCIAL CRIME PREVENTION:

A CASE STUDY OF CBZ HOLDINGS AND FBC HOLDINGS

1. What technologies does your bank currently use to detect and prevent financial crime?
2. How effective are these technologies in identifying suspicious transactions?
3. What challenges affect the use of these technologies in your bank?
4. How does your bank share financial intelligence or suspicious transaction information with FIU Zimbabwe or other relevant bodies?
5. What improvements would you recommend to strengthen financial crime prevention in your bank?

APPENDIX 4: TURNITIN REPORT

Gennah Gombe

GENNAH AI AND SIMILARITY CHECK

FI DISSERTATION PLAGIARISM CHECK

Document Details

Submission ID

trn:oid::2945:394523080

Submission Date

Jun 21, 2026, 2:57 PM GMT+2

Download Date

Jun 21, 2026, 4:14 PM GMT+2

File Name

GENNAH AI AND SIMILARITY CHECK.docx

File Size

752.8 KB

56 Pages

14,847 Words

87,347 Characters



Page 1 of 67 - Cover Page

Submission ID: trn:oid::2945:394523080



Page 2 of 67 - Integrity Overview

Submission ID: trn:oid::2945:394523080

11% Overall Similarity

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

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

- 121 Not Cited or Quoted 8%**
Matches with neither in-text citation nor quotation marks
- 52 Missing Quotations 3%**
Matches that are still very similar to source material
- 0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 6% Internet sources
- 3% Publications
- 9% Submitted works (Student Papers)

Gennah Gombe

GENNAH AI AND SIMILARITY CHECK

 FI DISSERTATION PLAGIARISM CHECK

Document Details

Submission ID	56 Pages
trnoid::2945:394523080	14,847 Words
Submission Date	87,347 Characters
Jun 21, 2026, 2:57 PM GMT+2	
Download Date	
Jun 21, 2026, 3:47 PM GMT+2	
File Name	
GENNAH AI AND SIMILARITY CHECK.docx	
File Size	
752.8 KB	

***% detected as AI**

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (i.e., our AI models may produce either false positive results or false negative results), so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.