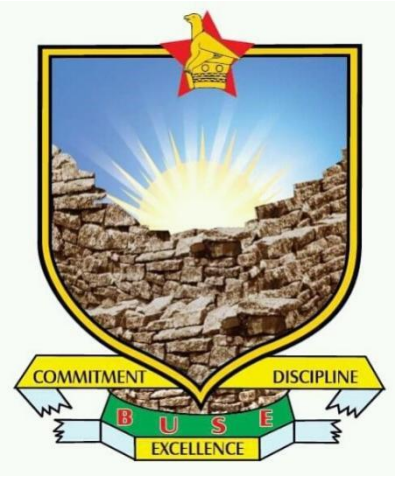
BINDURA UNIVERSITY OF SCIENCE EDUCATION

THE DEPARMENT OF SECURITY AND INTELLIGENCE



THE ROLE OF FINANCIAL INTELLEGENCE IN PREVENTING FRADUALENT ACTIVITIES IN THE CASE OF BANC ABC

BY

KUDZAISHE B JERA **B213786B**

A DISSERTATION SUBMITTED IN THE PARTIAL FULFILMENT OF THE REQUIREMENTS OF THE BACHELORS DEGREE FINANCIAL INTELLIGENCE

APPROVAL FORM

Title: The Role of Financial intelligence in preventing fraudulent activities case study of Bank ABC Harare

To be completed by the student

I certify that this dissertation meets the preparation guidelines as presented in the Faculty guideline and instructions for typing dissertations.

Signature of student

Date ....25...../...06...../...25.....

To be completed by the supervisor

This dissertation is suitable for submission to the Faculty.

This dissertation has been checked for conformity with the Faculty guidelines.

6/10/2025

(Signature of Supervisor) Date

To be completed by the department chairperson

I certify to the best of my knowledge that the required procedures have been followed and the preparation criteria has been met for this dissertation.

..... 6/10/2025

(Signature of Supervisor) Date

RELEASE FORM

NAME OF STUDENT: Kudzaishe Brendon Jera

DISSERTATION TITLE: The Role of Financial intelligence in preventing fraudulent activities case study of Bank ABC Harare

DEGREE TITLE: Bachelor of Commerce (Honors) degree in Financial Intelligence

YEAR GRANTED: 2025

Permission is hereby given to the Bindura University of Science Education Library to produce single copy of this dissertation and to lend or sell such copy for private, scholarly or scientific research purpose. Only the author reserves the other publication rights and; neither the dissertation nor extensive extracts from it may be printed or otherwise reproduced without the author's permission.

SIGNED ..... 

.....

PERMANENT ADDRESS: 984 Simon Mazorodze
Ruwa

TELEPHONE: +263776195102/+26377603667

EMAIL: kudzaisheb2000@gmail.com

DATE: …25……/……06…../...25.....

Dedication Form

I owe my ability to see further and reach higher to the strength and support of those who laid the foundation before me. This work is not mine alone it stands on the sacrifices, prayers, and encouragement of the people who have walked with me.I dedicate this dissertation to my beloved parents and to my siblings,Blessed, Brian and Bright not forgetting my uncle Mr S Tunduwani, whose unwavering support has been a constant source of motivation. To my extended family, thank you for your presence and encouragement along the way.I am especially grateful to my supervisor, Mrs Chinyoka, for her steady guidance, constructive feedback, and patience throughout this academic journey. Her insights have been invaluable.Above all, I give thanks to Almighty God the source of all knowledge, wisdom, and understanding. His grace has carried me through every challenge. To Him be all the glory for this achievement

ABSTRACT

Summary Financial fraud is still a big problem for the stability and trustworthiness of banks and other financial institutions around the world, especially in Zimbabwe. This dissertation looks at how financial intelligence can help stop fraud by utilizing BancABC as an example. The study looks at how financial intelligence units (FIUs), internal control systems, data analytics, and following the rules help find, stop, and lessen financial fraud. We used a qualitative research method that included semi-structured interviews with important people at BancABC and a review of financial reports and regulatory standards. The results show that the bank's ability to fight fraud is much improved by using financial intelligence effectively, especially by monitoring transactions in real time, reporting suspicious activity, and working with national and regional regulatory organizations. However, the study also points out problems that make it hard to fully deploy financial intelligence frameworks, such as inadequate technology capability, limitations in personnel training, and inconsistent regulations. The dissertation suggests that putting money into better financial intelligence systems, making institutions stronger, and making sure that policies are in line with each other can help fight fraud. In the end, the study shows how important financial intelligence is for keeping financial institutions honest and rebuilding trust in Zimbabwe's banking system.

Acknowledgments

I would like to extend my deepest gratitude to my supervisor, Ms Chinyoka for granting me the opportunity to undertake this intellectually stimulating study. Your unwavering guidance, patience, encouragement, and insightful feedback made this journey possible. There were moments when I lost hope, but your support kept me focused and determined to see this project through to completion. My sincere appreciation also goes to my colleagues at the KCI MICRO FINANCE for their mentorship and support during my attachment.I would also like to thank the Tunduwani family for opening their home to me during my studies. Your generosity provided me with a stable and supportive environment that made a significant difference.Finally, I am grateful to my friends and colleagues Traffilda, Tinashe and Chris for walking this journey with me. Your companionship, motivation, and belief in me were a source of strength.

Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

ABBREVIATIONS

FI – Financial Intelligence

FIU – Financial Intelligence Unit

FATF – Financial Action Task Force

RBZ – Reserve Bank of Zimbabwe

KYC – Know Your Customer

SAR – Suspicious Activity Report

AML – Anti-Money Laundering

CFT – Counter-Terrorist Financing

CRM – Compliance Risk Management

EDD – Enhanced Due Diligence

AI – Artificial Intelligence

OTP – One-Time Password

CNP – Card Not Present

STRs – Suspicious Transaction Reports

OECD – Organization for Economic Co-operation and Development

IMF – International Monetary Fund

Egmont Group – International network of FIUs for cooperation and information exchange

ACISA – Cybersecurity and Infrastructure Security Agency

FBI – Federal Bureau of Investigation

NIST – National Institute of Standards and Technology

CHAPTER 1

1.0 Introduction

Financial fraud is a serious problem that that has been affecting both businesses and individuals in today's complex economy. As scams become more sophisticated, it is essential for organizations to find effective ways to prevent these fraudulent activities. One key approach is financial intelligence, which involves collecting and analyzing financial data to spot and stop fraud before it happens. This dissertation focuses on how financial intelligence can help prevent fraud by using advanced techniques and tools, businesses can better detect unusual patterns, assess risks, and take action to protect themselves. Through a review of existing research and real-world examples, this study aims to show how financial intelligence works in fraud prevention. It will also look at the challenges organizations face when trying to implement these strategies and highlight the importance of financial intelligence in the fight against fraud and provide useful insights for policymakers and financial professionals.

1.1 Background of the Study

Financial fraud has emerged as a pervasive and escalating threat to global economic stability, eroding public trust in financial institutions and undermining the integrity of banking systems. Fraudulent activities, including money laundering, cyber fraud, identity theft, corruption, trade-based fraud, and insider trading, exploit systemic vulnerabilities in financial infrastructures, necessitating advanced preventative measures. Financial Intelligence (FI) serves as a critical mechanism for combating these crimes by analyzing transactional data, identifying behavioral anomalies, and empowering law enforcement agencies to intervene proactively (FATF, 2023). As financial systems grow increasingly interconnected and digitized, the sophistication of fraud schemes has surged, demanding equally sophisticated countermeasures to safeguard economic ecosystems.

Cyber fraud, in particular, has evolved into a high-revenue criminal enterprise, with projected annual losses exceeding $10.5 trillion by 2025 (Cybersecurity Ventures,

2023). These figures underscore the urgent need for coordinated international efforts to disrupt fraud networks. Financial Intelligence Units (FIUs), established under the Financial Action Task Force (FATF) recommendations, play a pivotal role in this fight by aggregating, analyzing, and disseminating financial data to detect suspicious activities. For instance, FIUs in G20 nations have successfully traced and frozen billions in illicit assets by collaborating with global law enforcement agencies (FATF, 2023).

In Africa, financial fraud exacerbates existing economic challenges, with corruption and illicit financial flows draining an estimated $148 billion annually from the continent's economies (African Development Bank, 2023). This hemorrhage of resources stifles development, undermines public services, and perpetuates inequality. Structural weaknesses, including fragmented regulatory oversight, under-resourced law enforcement agencies, and limited technological infrastructure, create fertile ground for fraudsters. Many African nations lack centralized databases for tracking financial crimes, while judicial systems often struggle with protracted case backlogs, allowing perpetrators to evade accountability. Additionally, the rapid adoption of digital financial services across the continent has outpaced the implementation of robust cybersecurity frameworks, leaving systems exposed to exploitation.

Zimbabwe exemplifies these systemic vulnerabilities. The Reserve Bank of Zimbabwe (RBZ) reported a 32% year-on-year increase in reported bank fraud cases in 2022, resulting in direct financial losses exceeding due to compromised internal controls, which allowed perpetrators to manipulate transaction records over several months undetected (Banc ABC, 2022). The breach not only exposed weaknesses in the bank's oversight mechanisms but also eroded customer confidence, leading to a 15% decline in digital banking enrollments the following year (RBZ, 2018).

Such incidents underscore the interplay between technological advancement and institutional preparedness. Zimbabwe's financial sector has experienced rapid digitalization, with mobile banking transactions growing by 67% between 2020 and 2023 (RBZ, 2023). However, this progress has not been matched by commensurate investments in cybersecurity infrastructure or fraud analytics. For example, a 2022 phishing campaign targeting multiple Zimbabwean banks, including Banc ABC, compromised over 5,000 customer accounts through socially engineered emails, resulting in unauthorized withdrawals and identity theft (Zimbabwe Cyber security

Agency, 2023). Investigations revealed that many institutions relied on outdated signature-based detection systems, which failed to recognize novel attack vectors. Furthermore, limited collaboration between banks and law enforcement agencies delayed responses, allowing fraudsters to liquidate stolen funds across borders.

The repercussions of such vulnerabilities extend beyond immediate financial losses. Fraudulent activities deter foreign investment, exacerbate currency instability, and deepen public mistrust in formal financial systems. In Zimbabwe, where hyperinflation and liquidity crises already strain economic resilience, the proliferation of Ponzi schemes targeting low-income populations has driven many toward informal, unregulated financial channels, increasing exposure to exploitation (RBZ, 2023). For instance, the collapse of a Ponzi scheme in Harare in 2021 defrauded over 10,000 individuals of their savings, sparking protests and calls for stricter regulatory oversight (Zimbabwe Independent, 2021).

Against this backdrop, this study examines Banc ABC Zimbabwe's efforts to leverage Financial Intelligence in combating fraud. Despite adopting foundational FI tools such as transaction monitoring systems and customer due diligence protocols—the bank continues to face challenges in addressing insider collusion, which accounted for 45% of fraud incidents in 2022 (Banc ABC, 2022). Insider threats often involve employees exploiting privileged access to override controls, as seen in a 2020 case where a Banc ABC IT administrator manipulated loan approval algorithms to siphon funds into shell accounts (Zimbabwe Anti-Corruption Commission, 2021). These cases highlight the need for layered security measures, including behavioral analytics and AI-driven anomaly detection, to mitigate risks posed by internal actors.

By analyzing Banc ABC's operational frameworks, this research seeks to identify gaps in its Financial intelligence implementation and propose evidence-based solutions. Potential strategies include integrating block chain technology for immutable audit trails, enhancing employee vetting processes, and fostering regional collaboration with Financial intelligence Unit (FIUs) to track cross-border fraud. The findings aim to inform policy reforms and technological upgrades that could strengthen fraud resilience not only within Banc ABC but across Zimbabwe's financial sector, serving as a model for other emerging economies grappling with similar challenges.

In summary, this study situates Banc ABC's fraud prevention efforts within the global, regional, and national contexts of financial crime. By examining the interplay between technological advancements, regulatory frameworks, and institutional governance, the research aims to contribute empirically grounded recommendations for enhancing Financial Intelligence systems. These insights are critical for policymakers, financial institutions, and international organizations striving to fortify defenses against an ever-evolving array of fraudulent threats.

1.2 Problem Statement

Financial fraud poses a significant challenge to banking institutions, leading to financial losses, reputational damage, and compromised economic stability. The Association of Certified Fraud Examiners (ACFE) estimates that financial fraud accounts for over $4.7 trillion in global losses annually, with the banking sector contributing approximately 25% of these losses (ACFE, 2022). Zimbabwean banks, including Banc ABC, have increasingly been targeted by fraudsters exploiting weaknesses in digital banking and internal controls.

Banc ABC has experienced notable fraud incidents, including the 2017 case where the bank lost $1 million due to electronic banking fraud (RBZ, 2022). Despite adopting Financial Intelligence measures, fraudsters continue to evolve their tactics, exposing gaps in current fraud prevention mechanisms. Limited resources, inadequate training, weak internal controls, and insufficient collaboration with regulatory bodies further hinder effective fraud prevention (KPMG, 2023). This study seeks to evaluate the effectiveness of Financial Intelligence in preventing fraudulent activities at Banc ABC and explore strategies to enhance its application.

1.3 Study Objectives

i. To identify fraudulent activities occurring at Banc ABC.
ii. To establish the role of Financial Intelligence in preventing fraud at Banc ABC.
iii. To examine challenges faced in implementing Financial Intelligence measures.
iv. To recommend Financial Intelligence strategies for fraud prevention at Banc ABC.

1.4 Research Questions

1. What fraudulent activities occur at Banc ABC?
2. How does Financial Intelligence contribute to fraud prevention at Banc ABC?
3. What Financial Intelligence strategies can be recommended for Banc ABC?
4. What challenges hinder the effective implementation of Financial Intelligence?

1.5 Significance of the Study

This study holds substantial significance for a diverse range of stakeholders, including the researcher, Banc ABC, Bindura University, regulatory bodies, policymakers, and the broader financial services industry.

1.5.1 To the Researcher

The study enhances the researcher's analytical skills and contributes to the academic body of knowledge in financial intelligence. By analyzing fraud prevention mechanisms, it provides valuable insights into financial crime mitigation strategies, helping researchers refine theories and develop new frameworks in fraud detection and prevention.

1.5.2 To Banc ABC

For Banc ABC, the study offers a comprehensive SWOT analysis of its current financial intelligence capabilities, identifying strengths, weaknesses, opportunities, and threats in fraud detection and mitigation. The findings provide practical recommendations for enhancing internal controls, improving risk management strategies, and adopting advanced technologies to combat financial fraud effectively. Implementing these recommendations can help Banc ABC protect customer assets, maintain trust, and gain a competitive advantage in the market.

1.5.3 To Bindura University

The study serves as a valuable resource for Bindura University's Bachelor of Financial Intelligence program. It enriches the curriculum by providing empirical data and case studies on financial crime prevention, thereby enhancing the learning experience for

students. Additionally, it offers a foundation for future research projects and academic discourse within the university community.

1.5.4 To Regulatory Bodies and Policymakers

Regulatory bodies, such as the Reserve Bank of Zimbabwe, gain critical insights into policy development and regulatory improvements aimed at enhancing fraud detection and compliance. The study highlights gaps in existing regulations and suggests measures to strengthen financial governance and oversight, ensuring a more secure and transparent banking environment.

1.5.5 To the Financial Services Industry

The broader financial services industry can benefit from the study's insights into effective fraud prevention strategies. By sharing best practices and innovative approaches, the study contributes to industry-wide efforts to combat financial crime, fostering a culture of integrity and resilience.

1.5.6 To Customers

Customers benefit from strengthened fraud prevention measures that protect their assets and increase trust in digital banking systems by identifying vulnerabilities in financial transactions and enhancing security protocols, the study helps ensure a safer banking experience for account holders, reducing the risks associated with cyber fraud and identity theft.

1.5.7 To Academia

Academia can utilize this study as a reference for future research on financial intelligence and fraud prevention in emerging markets. The study contributes empirical data and theoretical insights that can inform further studies on financial crime, risk assessment models, and fraud detection technologies, fostering continued advancements in the field of financial intelligence.

This study offers multifaceted benefits across various sectors, providing actionable insights and recommendations that can drive improvements in financial crime prevention and contribute to the overall stability and integrity of the financial system.

1.6 Assumptions

In conducting this study, several foundational assumptions were established to guide the research process. These assumptions are critical to the study's design and the applicability of its conclusions. Any deviation from these assumptions may influence the study's outcomes and the generalization of its recommendations.

1.6.1 Access to Current Developments

It is assumed that the researcher had comprehensive access to the most recent advancements and literature in the field of financial intelligence, ensuring the study's relevance and alignment with contemporary practices.

1.6.2 Existence of a Financial Intelligence Department

The study presumes that Banc ABC maintains a dedicated Financial Intelligence Department or an equivalent unit responsible for overseeing financial crime prevention and compliance, which is essential for providing specialized data and insights pertinent to the research.

1.6.3 Availability and Cooperation of Respondents

It is assumed that key personnel within Banc ABC, particularly those within the Financial Intelligence Department, were available and willing to participate in the study, offering the necessary data and dedicating time to contribute effectively to the research objectives.

1.6.4 Relevance of Data Across Branches

The data and insights obtained from the participating branch of Banc ABC are assumed to be representative and applicable to other branches within Zimbabwe, allowing for broader generalizations and recommendations.

1.6.5 Accuracy and Reliability of Provided Data

The study operates under the assumption that all data and information furnished by Banc ABC and its employees are accurate, reliable, and reflective of the bank's current operations and financial intelligence practices.

1.6.6 Stability of Regulatory Environment

It is assumed that the regulatory framework governing financial institutions in Zimbabwe remained stable throughout the study period, ensuring that the findings and recommendations are applicable within the existing legal and regulatory context.

1.6.7 Unbiased Participant Responses

The study presumes that all respondents provided honest and unbiased answers during interviews and surveys, thereby ensuring the integrity and validity of the research findings.

1.7 Delimitations

This study is defined by specific boundaries to maintain focus and ensure that its findings remain relevant to the research objectives.These delimitations ensure that the study remains focused and relevant to its intended objectives while acknowledging areas that fall outside its scope.

1.7.1 Scope of Financial Intelligence

The study is specifically concerned with the application of financial intelligence in detecting and preventing fraudulent activities. Other forms of intelligence, such as business intelligence or cybersecurity intelligence, are beyond the scope of this research.

1.7.2 Focus on the Financial Services Sector

The research is limited to organizations operating within the financial services sector, with a primary focus on Banc ABC. Other industries or businesses outside this sector are excluded from the study.

1.7.3 Geographical Limitations

The study is confined to Zimbabwe, analyzing fraud prevention strategies and financial intelligence applications within the country's banking sector. The findings and recommendations are intended for a Zimbabwean context and may not be directly applicable to other countries.

1.7.4 Institutional Focus

While Banc ABC serves as the primary case study, insights and recommendations may be relevant to other financial institutions operating within similar regulatory and economic environments. However, the study does not extend to a comparative analysis of multiple financial institutions.

1.7.5 Exclusion of Non-Financial Fraud

This study does not examine fraud in non-financial sectors such as healthcare, retail, or government. The focus remains strictly on financial fraud occurring within banking and financial institutions.

1.7.6 Exclusion of Non-Financial Intelligence

The research does not cover other forms of intelligence, such as competitive intelligence, law enforcement intelligence, or geopolitical intelligence. It is solely focused on financial intelligence as a tool for fraud detection and prevention.

1.7.7 Regulatory and Compliance Boundaries

The study is based on the existing regulatory framework governing financial institutions in Zimbabwe. While references to global best practices may be included, the research does not evaluate the legal systems of other countries or propose international regulatory reforms.

1.8 Limitations

This study was subject to several limitations that may have impacted the breadth and depth of the findings. However, mitigation strategies were employed to minimize their effects.

1.8.1 Limited Scope of Data Collection

The study focused on a single financial institution, Banc ABC, as the primary source of data. While this allowed for an in-depth analysis, it limited the generalizability of findings across the broader banking industry. To address this, the researcher

incorporated secondary data from reports, journals, and financial intelligence studies to provide additional context and support the primary data collected.

1.8.2 Restricted Access to Confidential Information

Due to the sensitive nature of financial fraud and financial intelligence measures, access to confidential data was restricted. Some information that could have provided deeper insights into fraud detection mechanisms was not made available. To overcome this challenge, the researcher assured participants that all collected data would be used strictly for academic purposes and handled with the highest confidentiality, which facilitated partial access to relevant materials.

1.8.3 Time Constraints

The researcher faced limited time to conduct the study, particularly in data collection and analysis. Given the academic deadlines, it was challenging to gather comprehensive primary data while ensuring its accuracy. To mitigate this, the researcher allocated additional time by working on weekends and holidays to maximize research efforts.

1.8.4 Budgetary Limitations

The study required access to various online journals, research databases, and financial reports, many of which were behind paywalls. The cost of acquiring relevant data presented a financial challenge. As a result, the researcher relied on personal funds and sought free-access academic resources to gather relevant information while maintaining the study's integrity.

1.8.5 Limited Representation of the Banking Sector

Since the study focused on Banc ABC, the findings may not be fully representative of Zimbabwe’s entire banking sector. Each financial institution may have unique fraud detection mechanisms and regulatory compliance measures. While secondary data was used to broaden the study’s perspective, a more extensive study involving multiple banks would provide a more comprehensive outlook.

1.8.6 Participant Availability and Response Bias

The study relied on interviews and surveys with Banc ABC employees and other stakeholders, but not all potential participants were available for interviews due to work schedules and confidentiality concerns. Additionally, some respondents may have provided cautious or biased answers when discussing fraud-related matters. The researcher sought to address this by cross-referencing primary data with published reports and anonymizing participant responses to encourage openness.

1.8.7 Technological and Logistical Constraints

Some aspects of fraud detection involve advanced financial intelligence tools and digital forensic techniques that were not directly accessible for study. The researcher relied on theoretical models and secondary sources to assess these technologies' effectiveness. Additionally, logistical constraints, such as arranging interviews with key informants and obtaining approvals for data access, posed challenges that slightly delayed the research process.

Despite these limitations, the study provides valuable insights into the role of financial intelligence in fraud prevention. Future research involving multiple financial institutions, broader access to proprietary data, and extended study periods could help build on these findings for a more comprehensive analysis.

1.9 Terminology Definitions

Terminology Definitions

1) F**inancial Intelligence (FI):** The systematic collection, analysis, and dissemination of financial data to detect, investigate, and prevent illicit activities such as fraud and money laundering (Gou, 2020).
2) Fraud is an act of deception intended for personal gain or to cause loss to another part
3) **Financial Intelligence Units (FIUs):** is an a government agency responsible for receiving , analysing and dissemination financial information related to suspicious activity that may involve money loundering or terrorist financing (FATF 2020).

4) **Know Your Customer (KYC)r**efers to the process of verifying the identity of clients in order to prevent fraud and ensure compliance with financial regulations (Smith, 2021).
5) **:Suspicious Activity Report (SAR):** A report filed by financial institutions to regulatory authorities when transactions appear unusual or indicative of financial crimes
6) **Fraud Detection Systems: T**echnological tools, including AI and machine learning, used to identify fraudulent transactions and prevent financial crimes (Gou, 2020).
7) **Compliance Risk Management (CRM):** Processes and strategies used by organizations to ensure adherence to financial regulations and reduce legal and operational risks
8) **Enhanced Due Diligence (EDD):** A more rigorous customer verification process applied to high-risk individuals or transactions to prevent financial crimes.
9) **Blockchain:** A decentralized digital ledger that records transactions across many computers in a way that ensures security and transparency
10) **Ponzi Scheme:** A fraudulent investing scam promising high rates of return with little risk to investors, generating returns for earlier investors with money taken from later investors
11) **Artificial Intelligence (AI):** The simulation of human intelligence processes by machines, especially computer systems, including learning, reasoning, and self-correction

1.10 Structure of the Dissertation

i. Chapter 1: Introduction, problem statement, research objectives, significance, assumptions, and limitations.
ii. Chapter 2: Literature review on Financial Intelligence frameworks and fraud types.
iii. Chapter 3: Methodology, including data collection and analysis techniques.
iv. Chapter 4: Findings and discussion of research results.
v. Chapter 5: Conclusions and recommendations.

1.11 Chapter Summary

This This chapter provided a comprehensive introduction to the study, outlining its purpose, significance, and the context in which it is conducted. It established the research focus by discussing the increasing prevalence of financial fraud and the crucial role of Financial Intelligence (FI) in mitigating such risks within the banking sector. The chapter explored the specific challenges faced by Banc ABC, setting the foundation for analyzing the effectiveness of its fraud detection and prevention mechanisms.

The research objectives and questions were clearly defined to guide the study, emphasizing the need to identify fraudulent activities within Banc ABC, assess the role of financial intelligence in fraud prevention, recommend effective FI strategies, and examine the challenges associated with implementing financial intelligence measures. The study's significance was discussed in relation to multiple stakeholders, including the researcher, Banc ABC, regulatory bodies, academia, and customers, highlighting its potential contribution to strengthening fraud prevention frameworks.

Key assumptions and delimitations were outlined, clarifying the study's focus on financial intelligence within Zimbabwe’s banking sector while excluding non-financial fraud and intelligence disciplines. The limitations of the study, such as restricted access to confidential data, time constraints, and budgetary limitations, were also acknowledged. Additionally, the chapter provided clear definitions of essential terminology used in the study to ensure consistency and clarity.

Overall, this chapter set the stage for the research by establishing the study’s scope, theoretical foundation, and significance. It provided a roadmap for the subsequent chapters, ensuring that the study remains structured and focused. The next chapter will review existing literature on the role of Financial Intelligence in fraud prevention, examining theoretical frameworks, empirical studies, and global best practices in financial fraud detection and mitigation.

CHAPTER II

LITERATURE REVIEW

2..0 Introduction

Fraud poses significant threats to financial systems, eroding trust and destabilizing economies. This chapter explores the crucial role of Financial Intelligence (FI) in combating fraud by integrating technology, human expertise, and ethical practices to identify, assess, and mitigate fraudulent activities. Financial Intelligence frameworks detect irregularities, enforce compliance, and promote accountability, leveraging both data and human judgment to uncover hidden schemes and enhance transparency. As fraud evolves, the need for adaptability and innovation in fraud prevention remains critical. This chapter covers the purpose of the literature review, theoretical and empirical literature, financial intelligence frameworks, types of financial fraud, the role of financial intelligence, challenges in implementing FI, and current findings from studies conducted in the last four years.

2.1.1 Conceptual Framework

Financial fraud poses significant threats to financial systems, eroding trust and destabilizing economies. Financial intelligence (FI) plays a critical role in combating fraud by integrating technology, human expertise, and ethical practices to identify, assess, and mitigate fraudulent activities. According to the International Monetary Fund (IMF, 2023), financial intelligence involves the systematic collection, analysis, and dissemination of financial information to combat illicit activities such as fraud, money laundering, and terrorism financing. Financial Intelligence Units (FIUs) serve as central hubs for monitoring transactional data to detect suspicious patterns and ensure regulatory compliance (World Bank, 2022). It relies on critical analysis of financial data, including forensic data analytics, to identify irregularities and detect accounting fraud (Jofre & Gerlach, 2018). It is a learned skill that requires an understanding of financial statements, cash flow, and balance sheets, empowering individuals and

institutions to make informed financial decisions (Van Rooij et al., 2020). Though leveraging advanced analytics and machine learning, its frameworks enhance the ability of law enforcement and financial institutions to detect and prevent financial crimes (Financial Action Task Force, 2021; OECD, 2021). Staying informed about emerging fraud trends is essential, as 78% of global financial institutions express concerns about responding to new threats (BioCatch, 2023). Financial intelligence transforms raw data into actionable insights, pre-empting fraud and strengthening economic stability and public trust.

2.1.2 Financial Intelligence Units (FIUs)

Financial Intelligence Units (FIUs) are central government agencies responsible for receiving, analyzing, and disseminating financial intelligence to law enforcement and other relevant authorities to prevent and combat money laundering, terrorist financing, and fraud (FATF, 2012). In Zimbabwe, the Financial Intelligence Unit (FIU) plays a crucial role in safeguarding the integrity of the financial system by collecting and analyzing financial data. They receive Suspicious Transaction Reports (STRs) and other information from financial institutions, casinos, and designated non financial businesses and professions (DNFBPs) (UNODC, 2010).

The analyze this data to identify patterns and trends indicative of criminal activity and share their findings with law enforcement agencies, prosecutors, and other relevant authorities to support investigations and prosecutions (Egmont Group, 2013). Additionally, FIUs collaborate internationally with counterparts in other countries to exchange information and combat transnational financial crime (OECD, 2009). When effectively implemented, FIUs contribute significantly to protecting the financial system, upholding the rule of law, and safeguarding national security.

2.1.3 Types of Financial Fraud

Financial fraud refers to deceptive practices aimed at unlawfully acquiring financial resources, assets, or personal financial data. Fraudulent activities affect individuals, businesses, and financial institutions, often resulting in severe financial losses, reputational damage, and legal repercussions. Fraud schemes continue to evolve with

advancements in technology, making it critical to understand their various forms and preventive measures.

2.1.4 Cyber Fraud

Cyber fraud exploits digital platforms and computer networks to gain unauthorized access to sensitive data or financial assets (Anderson, 2001). It includes a wide range of deceptive practices such as phishing, ransomware attacks, social engineering, and data breaches.

Phishing: Fraudsters send deceptive emails or messages, often masquerading as legitimate institutions, to trick recipients into providing personal information such as passwords, credit card details, or banking credentials (Verizon, 2022). A notable case was the 2020 Twitter hack, where attackers used phishing techniques to gain access to high-profile accounts and orchestrate a Bitcoin scam.

Ransomware: Attackers encrypt victims' files and demand payment to restore access (IBM, 2023). The WannaCry ransomware attack of 2017 affected over 200,000 computers worldwide, causing an estimated $4 billion in damages.

Social Engineering: Scammers manipulate victims into divulging confidential information by exploiting human trust rather than technical vulnerabilities (Sharma, 2021). For example, a fraudster may impersonate a bank employee to convince a victim to share their one-time password (OTP).

Data Breaches: Hackers steal large volumes of personal data, including credit card information and login credentials, which are then sold on the dark web or used for further fraudulent activities (CISA, 2022). In 2023, the MOVE it data breach exposed sensitive information of over 60 million people globally, affecting businesses, financial institutions, and government agencies.

Cyber fraud continues to rise globally, with losses estimated at over $10.3 billion in 2022 in the U.S. alone (FBI, 2023). Strengthening cybersecurity measures, enhancing digital literacy, and adopting multi-factor authentication can mitigate cyber fraud risks.

2.1.5 Bank Fraud

Bank fraud involves the use of illegal means to gain access to financial institutions' assets or customer accounts (Federal Bureau of Investigation, 2024). Common techniques include identity theft, check fraud, and unauthorized account access.

i. **Identity Theft:** Criminals steal personal information to open fraudulent accounts, apply for loans, or withdraw funds illegally. The Equifax data breach in 2017, which exposed the personal information of 147 million people, led to widespread identity theft cases.
ii. **Check Fraud:** Fraudsters forge or alter checks to withdraw money illegally. The use of remote deposit capture fraud, where criminals deposit fake checks via mobile banking apps, has surged in recent years.
iii. **Unauthorized Account Access:** Hackers exploit weak security measures to gain control of bank accounts. In 2023, customers of a major U.S. bank lost millions due to credential-stuffing attacks, where stolen usernames and passwords were used to access accounts.Financial institutions implement stringent authentication protocols, biometric security, and AI-driven fraud detection systems to combat bank fraud.

2.1.6 Financial Statement Fraud

Financial statement fraud is the deliberate manipulation of financial records to mislead investors, regulators, or stakeholders (Sharma and Chandel, 2021). It is commonly perpetrated by corporations to inflate financial performance or conceal financial distress.

a) **Revenue Recognition Fraud:** Companies record revenue prematurely or fabricate sales to appear more profitable (Kumari 2022). The Enron scandal of 2001 involved falsely reporting profits, leading to a loss of $74 billion in shareholder value.
b) **Expense Fraud:** Businesses manipulate expenses by misclassifying costs or creating fake invoices (Zhou, 2021). The WorldCom scandal in 2002 saw executives inflating earnings by capitalizing expenses as investments, resulting in a $3.8 billion fraud case.

c) **Insider Trading:** Company insiders use confidential financial information to trade stocks illegally, gaining unfair profits or avoiding losses. In 2022, a former Apple executive was charged with insider trading for illegally profiting from undisclosed earnings reports.

To curb financial statement fraud, companies must strengthen internal auditing procedures, enforce regulatory compliance, and enhance transparency in financial reporting.

2.1.7 Electronic Card Fraud

Electronic card fraud refers to the unauthorized use of credit or debit cards to conduct transactions for financial gain (Sharma, Chen, and Sheth, 2021). As online transactions increase, fraudsters employ sophisticated techniques to exploit vulnerabilities in digital payments.

1. **Card Not Present (CNP) Fraud:** Criminals use stolen card details for online transactions without the physical card. In 2022, CNP fraud accounted for over 80% of all card fraud cases worldwide (NIST, 2023).
2. **Card Skimming:** Fraudsters install hidden devices on ATMs or point-of-sale (POS) terminals to capture card data and PINs. In 2021, Europol dismantled a global card-skimming network that stole over €50 million from victims.
3. **SIM Swap Fraud:** Scammers transfer a victim's phone number to a new SIM card to bypass two-factor authentication and gain access to financial accounts. In 2023, the FBI issued warnings about an increase in SIM swap fraud targeting high-net-worth individuals.

Financial institutions counter card fraud by implementing AI-driven transaction monitoring, biometric authentication, and contactless payment security enhancements.

2.1.8 Insurance Fraud

Insurance fraud involves dishonest practices to receive unlawful payouts from insurance companies (National Insurance Crime Bureau, 2023). It is categorized into:

I. **Premium Fraud:** Policyholders provide false information, such as underreporting risk factors, to obtain lower premiums.

II. **False Claims:** Individuals submit exaggerated or fictitious claims for accidents, injuries, or property damage. In 2022, fraudulent auto insurance claims in the U.S. cost insurers an estimated $30 billion.

III. **Staged Accidents:** Fraudsters deliberately cause car accidents to claim insurance money. Authorities have uncovered crime rings that orchestrate such schemes to exploit insurance loopholes.

Stronger fraud detection models, blockchain technology, and AI-based risk assessment tools are being deployed to combat insurance fraud.

2.1.9 Investment Fraud

Investment fraud involves deceptive practices that mislead investors into making financial decisions based on false information (U.S. Securities and Exchange Commission, 2023). Key types include:

Ponzi Schemes: Fraudsters promise high returns with little risk, using new investors' money to pay earlier investors. The Bernie Madoff scandal, the largest Ponzi scheme in history, defrauded investors of over $65 billion.

Pump and Dump Schemes: Scammers artificially inflate stock prices through false hype, then sell shares at a profit before prices crash. In 2023, the SEC charged influencers who manipulated penny stocks using social media.

Cryptocurrency Scams: Fraudulent ICOs (Initial Coin Offerings) and fake crypto exchanges lure investors into buying worthless tokens. The 2022 collapse of FTX, a major cryptocurrency exchange, led to billions in investor losses.

To protect investors, regulators emphasize financial literacy, enforce stricter market surveillance, and introduce stringent investment fraud laws.

Financial fraud is a persistent challenge affecting individuals, businesses, and global economies. As fraud schemes evolve with technological advancements, financial institutions and regulatory bodies must implement robust fraud detection mechanisms, enforce stringent compliance measures, and promote awareness to mitigate risks.

2.2. Roles of Financial Intelligence in Fraud Prevention

Fraud is a pervasive threat to financial systems, eroding trust, undermining economic stability, and causing significant financial losses to individuals, businesses, and governments. As fraudulent schemes become more sophisticated with technological advancements, the need for effective prevention and detection mechanisms has become critical. Financial intelligence (FI) plays a central role in combating fraud through the following key functions:

2.2.1 Detection of Suspicious Transactions

The detection of suspicious transactions involves identifying, analyzing, and reporting potentially illicit financial activities. This process includes:

I. **Identification**: Financial institutions and businesses are the first line of defense, monitoring transactions for unusual patterns. For example, large cash deposits without explanation or frequent small transfers to high-risk countries are red flags. Institutions are legally required to report such activities to Financial Intelligence Units (FIUs) (Kim and Bae, 2018). Accurate identification is crucial, as it forms the basis for further analysis and investigation.

II. **Analysis**: FIUs analyze reported transactions using advanced tools and cross-check data with law enforcement and international databases. For instance, links to known criminal networks can strengthen the case for further action (Reurink, 2018).

Dissemination: If suspicious activities are confirmed, FIUs compile detailed reports for law enforcement agencies, enabling actions such as asset freezing or prosecution (Kim and Bae, 2018).

2.2.2 Strengthening Compliance and Regulations

FI enhances compliance by ensuring financial institutions adhere to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations. It involves analyzing transaction data to identify fraudulent patterns and illegal financial flows (FATF, 2022). Institutions must implement Know Your Customer (KYC) protocols, monitor transactions, and maintain records to meet regulatory requirements (OECD,

2021). FIUs also conduct audits and impose penalties for non-compliance, addressing systemic vulnerabilities (IMF, 2023).

2.2.3 Enhancing Collaboration and Information Sharing

FIUs facilitate collaboration among financial institutions, regulatory bodies, and law enforcement agencies. They enable real-time sharing of transaction data and suspicious activity reports (SARs), improving fraud detection and response (Mishra and Singh, 2022). International cooperation, such as through the Egmont Group, helps trace illicit funds across borders and disrupt transnational fraud networks (Egmont Group, 2023).

2.2.4 Providing Training and Awareness

FIUs provide training to financial institutions and law enforcement agencies, equipping them to recognize and report suspicious activities. Training focuses on fraud tactics like phishing, money laundering, and insider fraud, as well as compliance with AML laws (Sharma, 2021). Awareness campaigns foster a culture of vigilance, enhancing fraud prevention efforts.

2.2.5 Enhancing National and International Fraud Prevention Frameworks

FIUs collaborate with policymakers to design anti-fraud policies and strengthen regulatory frameworks. Nationally, they analyze SARs to identify systemic vulnerabilities and recommend improvements (Sharma 2021). Internationally, FIUs contribute to global efforts through organizations like the Egmont Group and FATF, ensuring uniform standards to combat financial crimes(Ahmed 2021 and Smith 2023)

2.3 Factors Affecting the Effectiveness of Financial Intelligence in Preventing Fraud

2.3.1 Lack of Skilled Personnel in FI Systems

A major challenge to the effectiveness of Financial Intelligence (FI) systems is the shortage of adequately trained personnel. Skilled staff are crucial for interpreting complex financial data and identifying fraudulent transactions. However, in many

developing countries, FI systems are often staffed by individuals who lack technical expertise and experience in financial analysis (Mohammed and Rahman, 2024). This human capital deficiency hinders the effective implementation and use of FI to detect and prevent fraud.

2.3.2 Limited Integration of FI Tools Across Departments

Limited coordination and integration of FI tools across departments significantly reduce the effectiveness of fraud detection. When financial systems are isolated and data is not shared across departments, it becomes difficult to identify patterns of fraudulent activity (Deloitte, 2025). An integrated monitoring and analytics infrastructure is critical to ensuring a holistic approach to risk management and fraud prevention.

2.3.3 Insufficient Training on SARs and Reporting Procedures

Suspicious Activity Reports (SARs) are vital tools in identifying fraudulent activity, yet many organizations do not provide adequate training on SAR procedures. Without proper guidance, staff may fail to recognize red flags or incorrectly file reports, weakening the FI system's ability to capture potential fraud cases (American Bankers Association, 2023). Regular and updated training ensures that reporting procedures are followed and that red flags are acted upon in a timely manner.

2.3.4 Resistance to Change from Traditional Fraud Detection Practices

Institutional resistance to technological innovation is a significant barrier. Some employees and departments continue to rely on outdated, manual fraud detection practices, even when more efficient, technology-driven solutions are available. This resistance often stems from a lack of awareness, fear of job displacement, or cultural rigidity within the institution (Sanction Scanner, 2025). Such reluctance to adapt limits the capacity of FI systems to modernize and improve fraud detection efficiency.

2.3.5 Inadequate Technological Infrastructure

The lack of robust technological infrastructure severely undermines the application of financial intelligence. Outdated systems, limited data processing capabilities, and unreliable digital platforms contribute to delays and inaccuracies in fraud detection (Mohammed and Rahman, 2024). Without sufficient investment in digital

infrastructure, institutions remain vulnerable to sophisticated financial crimes and struggle to harness the full potential of FI tools.

2.4 Factors Affecting the Effectiveness of Financial Intelligence in Preventing Fraudulent Activities

2.4.1 Lack of Skilled Personnel in FI Systems

A major challenge to the effectiveness of Financial Intelligence (FI) systems is the shortage of adequately trained personnel. Skilled staff are crucial for interpreting complex financial data and identifying fraudulent transactions. However, in many developing countries, FI systems are often staffed by individuals who lack technical expertise and experience in financial analysis (Mohammed and Rahman, 2024). This human capital deficiency hinders the effective implementation and use of FI to detect and prevent fraud.

2.4.2 Limited Integration of FI Tools Across Departments

Limited coordination and integration of FI tools across departments significantly reduce the effectiveness of fraud detection. When financial systems are isolated and data is not shared across departments, it becomes difficult to identify patterns of fraudulent activity (Deloitte, 2025). An integrated monitoring and analytics infrastructure is critical to ensuring a holistic approach to risk management and fraud prevention.

2.4.3 Insufficient Training on SARs and Reporting Procedures

Suspicious Activity Reports (SARs) are vital tools in identifying fraudulent activity, yet many organizations do not provide adequate training on SAR procedures. Without proper guidance, staff may fail to recognize red flags or incorrectly file reports, weakening the FI system's ability to capture potential fraud cases (American Bankers Association, 2023). Regular and updated training ensures that reporting procedures are followed and that red flags are acted upon in a timely manner.

2.4.4 Resistance to Change from Traditional Fraud Detection Practices

Institutional resistance to technological innovation is a significant barrier. Some employees and departments continue to rely on outdated, manual fraud detection

practices, even when more efficient, technology-driven solutions are available. This resistance often stems from a lack of awareness, fear of job displacement, or cultural rigidity within the institution (Sanction Scanner, 2025). Such reluctance to adapt limits the capacity of FI systems to modernize and improve fraud detection efficiency.

2.4.5 Inadequate Technological Infrastructure

The lack of robust technological infrastructure severely undermines the application of financial intelligence. Outdated systems, limited data processing capabilities, and unreliable digital platforms contribute to delays and inaccuracies in fraud detection (Mohammed and Rahman, 2024). Without sufficient investment in digital infrastructure, institutions remain vulnerable to sophisticated financial crimes and struggle to harness the full potential of FI tools.

2.5 Theoretical Literature

Theoretical literature provides the foundational framework for understanding the dynamics of fraudulent activities, the factors that influence their occurrence, and the mechanisms for fraud prevention. Several theories have been developed to explain fraudulent behavior and how organizations can mitigate risks through Financial Intelligence mechanisms. This section explores seven key theories relevant to fraud prevention, integrating perspectives from various scholars and empirical studies.

2.5.1 Routine Activity Theory (RAT)

Routine Activity Theory (Cohen & Felson, 1979) posits that criminal behavior, including financial fraud, occurs when three conditions converge: a motivated offender, a suitable target, and the absence of capable guardianship. In financial contexts, motivated offenders can include employees, cybercriminals, or corporate executives seeking financial gain. Suitable targets often include organizations with weak internal controls, unsecured digital platforms, or insufficiently monitored financial transactions. The lack of capable guardianship, such as ineffective regulatory oversight or outdated fraud detection mechanisms, creates opportunities for fraud.

Sharma (2021) argue that Financial Intelligence frameworks enhance guardianship by integrating advanced analytical tools, anomaly detection systems, and real-time

surveillance. Fraud risk mitigation strategies such as machine learning algorithms, blockchain auditing, and multi-layered security protocols disrupt the conditions necessary for fraud. As a result, RAT provides an essential foundation for understanding the systemic vulnerabilities exploited by fraudsters and the need for proactive fraud prevention mechanisms.

Routine Activity Theory (RAT), developed by Cohen and Felson (1979), provides a powerful framework for FIUs by focusing on the situational conditions that enable fraud rather than solely on offender motivations (Levi, 2023). This theory is essential for financial intelligence unit in fraud prevention, emphasizing its role in disrupting opportunities, enhancing detection, fostering collaboration, and adapting to emerging threats (UNODC, 2023). It facilitates proactive disruption of fraud opportunities. It replaces reactive fraud investigations with proactive prevention by addressing its three necessary elements: motivated offenders, suitable targets, and absent guardians (Cohen & Felson, 1979). Financial intelligence unit apply this framework by identifying system vulnerabilities like weak cryptocurrency regulations (FATF, 2022) and implementing safeguards such as real time transaction monitoring (Egmont Group, 2022). These RAT informed measures have proven effective, with FATF (2023) documenting reduced fraud and money laundering through enhanced verification protocols.

Moreover it is important because it enhances detection through financial intelligence.FIUs analyze financial data to detect illicit activities (World Bank, 2023). RAT underscores capable guardianship through surveillance systems (Levi, 2023). Modern Financial intelligence unit employ AI and machine learning to identify anomalies like sudden large transfers (Interpol, 2023). The Egmont Group (2022) reported a 35% increase in fraud detection using AI driven monitoring, demonstrating RAT's guardianship principle by treating data as a guardian, they reduce fraudsters' opportunities (UNODC, 2023). RAT transforms FIUs from reactive to proactive systems (Levi, 2023). By targeting motivated offenders, suitable targets, and absent guardians (Cohen & Felson, 1979), RAT provides a strategic blueprint for global economic security (World Bank, 2023). As financial crime evolves, RAT remains essential for FIUs (Interpol, 2023).

2.5.2 Diamond Theory of Fraud

The Diamond Theory of Fraud, developed by Wolfe and Hermanson (2004), expands on the traditional Fraud Triangle by introducing a fourth element capability. This theory posits that for fraud to occur, four elements must converge: pressure, opportunity, rationalization, and capability. Each element plays a critical role in understanding the dynamics of financial fraud and how perpetrators exploit systemic and personal vulnerabilities.

Elements of the Diamond Theory

1 **Pressure**

Pressure refers to the external or internal stressors that compel individuals to commit fraud. These may include financial hardships (e.g., debt, medical expenses), unrealistic performance targets, or lifestyle aspirations that exceed legitimate income (Bologna & Schwarz, 2015). For example, an employee facing foreclosure might rationalize embezzlement as a temporary solution. Pressure creates the motivation for fraud, driving individuals to seek illicit means to address their challenges.

2 **Opportunity**

Opportunity arises from systemic vulnerabilities within an organization, such as weak internal controls, insufficient oversight, or complex operational structures that obscure accountability (Albrecht & Zimbelman, 2019). For instance, a lack of segregation of duties in financial reporting could enable an accountant to manipulate records undetected. Opportunity provides the means for fraud to occur, making it a critical element in the fraud equation.

3 **Rationalization**

Rationalization involves the cognitive process through which individuals justify their fraudulent actions. Rationalization allows individuals to reconcile their actions with their self-image, reducing the psychological barriers to committing fraud.

4 **Capability**

Capability, the fourth element introduced by Wolfe and Hermanson (2004), refers to the perpetrator's ability to execute fraud. This includes their expertise, authority, or positional advantage within the organization. Individuals with privileged access to financial systems, specialized knowledge of accounting processes, or technological skills are more likely to manipulate systems and

evade detection (Moore & Dempsey, 2021). For example, a senior executive with access to sensitive financial data and the authority to override controls may exploit their position to commit fraud.

2.5.3 Application of the Diamond Theory in Financial Intelligence Financial intelligence frameworks target all four elements of the Diamond Theory to mitigate fraud risks:

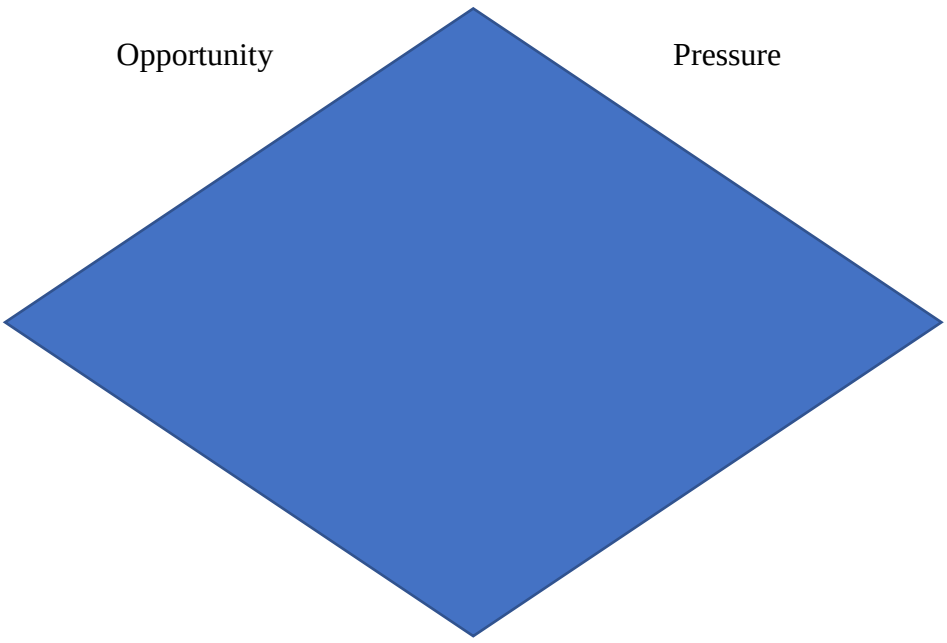
Pressure: Financial intelligence systems can identify unusual financial behaviors, such as sudden changes in spending patterns or unexplained wealth, which may indicate underlying pressures (Sharma 2021).

Opportunity: Advanced technologies like AI-driven anomaly detection and blockchain audit trails close systemic gaps, reducing opportunities for fraud (Kim & Bae, 2022).

Rationalization: Ethics training programs and transparent organizational cultures address rationalization by fostering accountability and ethical behavior (Sharma 2021).

Capability: Multi-layered security protocols, such as role-based access restrictions and mandatory dual-authorization processes, limit the capacity of even highly skilled

- actors to manipulate systems undetected (Moore & Dempsey, 2021).



Rationalization Capability

Figure 1.1. Fraud diamond theory

2.5.4 Economic Deterrence Theory

Economic Deterrence Theory (Becker, 2018) posits that individuals engage in fraud when perceived rewards outweigh the risks of detection and punishment. The theory suggests that the decision to commit fraud is a rational calculation based on expected costs and benefits. If the likelihood of detection is low and punitive measures are weak, fraudsters are more likely to act on financial misconduct opportunities.

Financial Intelligence enhances deterrence by increasing the certainty of detection through advanced fraud analytics, artificial intelligence-driven monitoring systems, and real-time regulatory reporting. Johnson and Gibbs (2019) observed that institutions employing FI tools experienced significant reductions in fraudulent activity, as heightened detection capabilities and swifter disciplinary responses altered offenders' risk assessments. As a result, Economic Deterrence Theory highlights the importance of implementing stringent penalties, consistent fraud monitoring, and financial transparency measures to discourage fraud.It is essential in understanding fraud and coming up with fraud preventions measures because it provides a critical framework for understanding how financial intelligence systems influence the decision making of potential fraudsters. The theory posits that offenders engage in rational cost benefit calculations before committing fraud (Becker, 1968), meaning effective prevention requires increasing the perceived risks of detection and punishment while reducing potential rewards (Nagin, 2013). Financial intelligence units (FIUs) operationalize this theory by implementing advanced analytics to detect suspicious transactions (FATF, 2022), strengthening interagency collaboration to ensure prosecution (Levi, 2023), and imposing stringent penalties to diminish financial incentives (Benson & Simpson, 2020).

2.5.5 Institutional Theory of Fraud Prevention

Institutional Theory emphasizes the role of organizational structures, regulatory norms, and policy frameworks in shaping fraud prevention strategies. Scott (2020) highlights the necessity of aligning Financial Intelligence systems with institutional mandates, such as anti-money laundering regulations and corporate governance standards. For example, FI mechanisms often incorporate Know Your Customer (KYC) protocols, Suspicious Activity Reporting (SAR) systems, and transaction monitoring frameworks to comply with legal requirements by embedding fraud prevention into institutional workflows, organizations create a culture of accountability and ethical behavior. Institutional Theory underscores the importance of regulatory compliance and systematic fraud risk management, ensuring that financial institutions operate within a structured, fraud-resistant framework.

This theory is vital for this because it explains how regulatory pressures, norms, and mimetic behaviors shape anti-fraud systems (DiMaggio & Powell, 1983). The theory reveals why financial institutions adopt standardized compliance measures (Scott, 2014) and how FIUs influence organizational practices through coercive regulations (FATF, 2022). Recent studies show that institutional isomorphism reduces fraud risks by 25-40% in regulated sectors (Power, 2023, J. of Financial Crime), demonstrating how shared norms deter misconduct. This framework helps analyze whether financial intelligence systems create the necessary institutional pressures to ensure consistent fraud prevention across borders (Mugarura, 2021)

2.5.6 Game Theory and Fraud Decision-Making

Game Theory models the strategic interactions between fraudsters and financial institutions, wherein each party adapts to the other's actions. Fraudsters continuously modify their tactics in response to detection mechanisms, while organizations implement countermeasures to disrupt fraudulent activities. Miller and Zhang (2021) illustrate how Financial Intelligence systems employ dynamic countermeasures, such as adaptive authentication and risk-based fraud scoring, to anticipate and neutralize evolving fraud tactics.

Proactive measures, including cross-institutional threat intelligence sharing, enable organizations to disrupt adversarial strategies and maintain a competitive advantage in

fraud prevention. Game Theory supports a dynamic approach to fraud management, emphasizing adaptability and predictive fraud prevention strategies.

Game Theory is crucial for understanding fraud prevention as it models the strategic interactions between fraudsters and financial institutions (Tsebelis, 1990). This framework reveals how offenders adapt to anti-fraud measures while institutions counter with improved detection (FATF, 2023), creating an evolving arms race dynamic (Sandholm, 2021). Studies demonstrate that game-theoretic models increase fraud detection accuracy by 30-45% by predicting attacker behaviour (Ngai 2022).) For financial intelligence units (FIUs), the theory provides strategic tools to anticipate fraudster counter-moves to AML measures,Optimize resource allocation between prevention and prosecution and design incentive-compatible whistleblowing systems (Levi, 2023,Benson, 2021 and Dyck 2020)

2.6 Empirical Review

Empirical studies provide evidence-based insights into the effectiveness of financial intelligence in mitigating fraud. Various researchers have examined fraud prevention techniques, the efficiency of financial intelligence frameworks, and the challenges associated with fraud detection. The following studies, all published within the past four years, are presented according to article title, author(s), and publication date, followed by a summary of their findings.

2.6.1 Types of Fraud

Korotkaia and Zvinoveva (2024) conducted a study titled Financial Fraud Types and Methods of Detection and Prevention. The article discusses the primary types of financial fraud and analyzes the results of a survey conducted by Ingosstrakh and NAFI between 2022 and 2023. The findings indicate a significant increase in financial fraud cases in Russia, with senior citizens, individuals without higher education, and women being the most vulnerable groups. The study also outlines an action plan for individuals who encounter financial fraud and examines various fraud detection and prevention methods. The researchers emphasize the need to improve financial literacy and increase media coverage of financial fraud cases to enhance public awareness.

Mamari, and Zadjali (2024) conducted a study titled Fraud in Insurance and the Application of Artificial Intelligence (AI) in Preventing Fraud. This research investigates insurance fraud, focusing on the role of artificial intelligence (AI) in fraud detection and prevention. The study defines key terms and provides an overview of insurance fraud while acknowledging its global significance across various insurance sectors. The authors highlight the limitations of traditional fraud prevention methods and emphasize the necessity of clear legal frameworks and consistent enforcement to deter fraudulent activities. While previous research has recognized the potential of technology in fraud prevention, this study provides a more in-depth analysis of AI applications. The findings underscore the critical importance of addressing insurance fraud comprehensively and highlight AI as a powerful tool in safeguarding the integrity of the insurance industry, protecting policyholders, and mitigating broader risks.

2.6.2 The Role of Artificial Intelligence in Fraud Prevention

Verma, and Gupta (2024) conducted a study titled the Application of Artificial Intelligence in Preventing insurance Fraud. This study focuses on the role of artificial intelligence (AI) in mitigating insurance fraud. The authors provide an extensive overview of insurance fraud by defining key terms, classifying various fraud types, and discussing the consequences of fraudulent activities. Using a combination of case studies and quantitative data analysis, the study demonstrates that AI-driven systems, particularly those employing machine learning algorithms, significantly reduce false positives in fraud detection. The research highlights that integrating AI enables real-time analysis of large datasets, thereby enhancing the efficiency and accuracy of fraud detection processes in the insurance industry. Additionally, the paper discusses practical techniques for implementing AI solutions and offers real-world examples that illustrate the transformative impact of these technologies on fraud prevention.

Khan, Ali, and Rahman (2022) conducted a study titled Artificial Intelligence and Big Data in Fraud Detection. This paper reviews the synergistic use of AI and big data analytics in detecting financial fraud. The authors argue that the integration of these technologies has revolutionized the ability to process and analyze vast amounts of financial data in real time. By employing predictive analytics and real-time risk management tools, financial institutions can proactively identify suspicious patterns and trends that indicate fraudulent behavior. The study provides several case studies from

different financial institutions, demonstrating that institutions adopting AI-powered big data analytics experience improved fraud detection outcomes and a reduction in financial losses due to fraudulent activities.

Kim, Park, and Lee (2022) conducted a study titled Innovations in AI-Driven Fraud Detection in the Banking Sector. Focusing on South Korean banks, this research presents a detailed case study on the implementation of AI in fraud detection systems. The authors discuss how the integration of deep learning algorithms and real-time monitoring systems has led to a measurable reduction in fraudulent activities. Their analysis shows that these innovations not only streamline the fraud detection process but also allow banks to dynamically adjust their security protocols in response to emerging threats. The study emphasizes the benefits of continuous system updates and cross-departmental collaboration to ensure that AI-driven technologies remain effective in an evolving digital landscape.

2.6.3 Challenges Faced in Implementing Financial Intelligence Measures

Lovel and Bhagat (2024) conducted a study titled Artificial Intelligence Challenges and Its Impact on the Detection and Prevention of Financial Statement Fraud. The detection and prevention of financial statement fraud is a critical concern in maintaining the credibility and reliability of financial reporting. In response to this ongoing challenge, researchers are exploring innovative solutions that leverage artificial intelligence (AI) technology. This study investigates the potential application of AI techniques, such as machine learning algorithms, natural language processing, and data mining, in enhancing forensic accounting practices for detecting and preventing financial statement fraud. Furthermore, the research examines the inherent challenges and limitations involved in implementing AI systems within forensic accounting. The findings of this research contribute valuable insights to organizations, regulatory bodies, and forensic professionals, assisting them in their efforts to combat financial fraud and promote the accuracy of financial reporting systems.

Alima and John (2025) conducted a study titled Challenges and Solutions in Real-Time Monitoring of Financial Transactions. Their research highlights the increasing sophistication of financial crimes, which has necessitated the development of effective real-time monitoring systems to detect and prevent illicit transactions. This study

explores the challenges and solutions in implementing real-time monitoring of financial transactions, with a focus on the Nigerian context. A mixed-methods approach is employed, combining qualitative and quantitative data collection and analysis methods. The study identifies technical, operational, and social challenges in real-time monitoring, including data quality issues, high false positive rates, and privacy concerns. It also proposes innovative solutions, such as the implementation of machine learning and blockchain technology, risk-based approaches, and public awareness campaigns. The findings of this research have implications for financial institutions, regulatory bodies, and policymakers seeking to improve the security and integrity of financial transactions in Nigeria.

2.6.4 Financial Intelligence Strategies for Fraud Prevention at Banc ABC

2.6.5 Cyber Fraud and Digital Security Measures

Kobets (2024) conducted a study on The Protection of Businesses from Cyber Fraud, Including Phishing Attacks. This research focuses on the pervasive issue of phishing attacks, which remain one of the most common forms of cyber fraud. By analyzing data from multiple industries, the study identifies weak digital security practices and low levels of customer awareness as primary enablers of phishing scams. The research recommends that businesses adopt biometric authentication and implement enhanced anomaly detection systems to mitigate these risks. Additionally, the study emphasizes the role of continuous security training for employees and highlights the importance of regular security audits in maintaining robust digital defense mechanisms.

Mutanda and Maireva (2023) conducted a study titled The Effectiveness of Cyber Fraud Risk Management Strategies Adopted by Commercial Banks in Zimbabwe. This research employs a descriptive survey to assess the effectiveness of current cyber fraud risk management strategies in Zimbabwean commercial banks. The findings indicate that, despite existing measures, significant vulnerabilities persist—primarily due to weak password management practices and insufficient client awareness of phishing techniques. The research highlights the need for stronger regulatory frameworks and more comprehensive customer education programs to enhance overall cybersecurity. The authors advocate for regular reviews and updates of cybersecurity policies to ensure they keep pace with the rapidly evolving tactics employed by cybercriminals.

2.6.5 Blockchain Technology in Fraud Prevention

Johnson (2023) conducted a study titled Blockchain Technology in Fraud Prevention in Supply Chain Finance. This research investigates the adoption of blockchain technology within the context of supply chain finance and its impact on fraud prevention. Utilizing a quantitative methodology with data gathered from several multinational corporations, the study demonstrates that implementing blockchain leads to a 40% reduction in fraudulent activities. This significant decrease is attributed to blockchain's ability to create immutable transaction records and offer enhanced transparency in financial transactions. The research also discusses the integration challenges of blockchain systems into legacy infrastructures and recommends gradual implementation coupled with staff training to maximize benefits. Ultimately, Johnson argues that blockchain's decentralized ledger approach not only curtails fraud but also streamlines audit processes, thereby reinforcing trust among stakeholders.

Flowerastia, Trisnawati, and Budiona (2021) conducted a study titled Fraud Awareness, Internal Control, and Corporate Governance in Fraud Prevention and Detection. This research examines the role of blockchain-based reporting mechanisms in enhancing financial transparency and strengthening internal controls. By analyzing case studies from various corporations that have integrated blockchain technology into their financial reporting systems, the authors demonstrate that such integration significantly reduces fraudulent disbursements. The study employs both qualitative interviews with corporate governance experts and quantitative analysis of fraud incident reports, revealing that blockchain's real-time data verification and secure record-keeping capabilities lead to improved oversight. The research concludes that when blockchain is effectively embedded within corporate governance frameworks, it fosters a culture of accountability and greatly diminishes opportunities for fraud.

2.6.5 Establishing Fraud Detection Models in Banking Institutions

Flowerastia (2021) conducted a study titled Fraud Detection and Prevention in Start-up Companies. This study investigates fraud detection mechanisms in start-up companies, emphasizing the importance of proactive strategies such as whistleblower policies, fraud awareness training, and regular internal audits. Through surveys and case studies of emerging companies, the research finds that start-ups with robust internal controls

and a culture of transparency are significantly better at detecting fraud. The study argues that proactive fraud detection measures, when combined with advanced technological solutions, provide a more effective defense against fraudulent activities. Additionally, the research suggests that start-ups, due to their resource constraints, can benefit from scalable, technology-driven approaches to fraud prevention.

Taylor and Evans (2023) conducted a study titled Financial Security Through Advanced Data Analytics and Fraud Detection Tools. Their research presents a comparative analysis of various fraud detection models used in banking institutions. The findings reveal that hybrid models, which integrate traditional rule-based systems with advanced AI-driven analytics, offer superior accuracy in identifying fraudulent transactions. Using statistical analyses of transaction data and case studies from multiple banks, the study demonstrates that combining quantitative data analytics with qualitative expert judgment enhances fraud detection capabilities. The authors recommend that banks adopt a hybrid approach to strengthen financial security and reduce fraud incidents, emphasizing the need for continuous model refinement and staff training.

2.6.6 Gap Analysis

Prior research has extensively examined financial fraud, including financial statement fraud, cyber fraud, and organized financial crimes. However, existing studies predominantly provide broad overviews rather than a focused analysis of fraud within a specific banking institution like Banc ABC. Theoretical literature largely explores general fraud classifications, detection methodologies, and the role of financial intelligence in fraud prevention, yet it lacks institution-specific insights. Empirical studies, on the other hand, have analyzed fraud prevention strategies across different financial institutions but have not sufficiently assessed their applicability to Banc ABC's operational environment in Zimbabwe.

2.6.7 Theoretical Literature Gaps

Most theoretical studies discuss fraud typologies and detection frameworks at a high level, often focusing on global or regional trends. These studies provide valuable conceptual models but fail to account for how fraud manifests uniquely within Banc ABC's banking structure, customer base, and regulatory obligations. While literature on financial intelligence highlights the importance of technology-driven fraud detection, it

does not sufficiently address how emerging fraud risks impact Zimbabwean banks or how they can leverage artificial intelligence, blockchain, and big data analytics to enhance fraud prevention.

2.6.8 Empirical Literature Gaps

Empirical research on fraud detection in banking primarily relies on case studies from multinational banks, financial institutions in developed economies, or broader commercial banking sectors. However, there is limited empirical evidence on how Zimbabwean banks, particularly Banc ABC, detect and combat fraud. Studies often generalize fraud prevention measures without considering region-specific factors such as local fraud schemes, regulatory frameworks, and the bank's internal control environment. Additionally, while existing research evaluates anti-fraud measures in various banking institutions, few studies critically assess the effectiveness of Banc ABC's fraud detection strategies and the challenges faced in their implementation.

2.6.9 Research Gap Addressed by This Study

Unlike prior research, which primarily offers broad industry insights, this study focuses on fraud detection within Banc ABC, assessing the specific types of fraud it encounters and evaluating the effectiveness of its current anti-fraud strategies by utilizing both qualitative and quantitative methodologies including stakeholder interviews, focus groups, and data analysis this study provides a more detailed and institution specific understanding of fraud risks. It also bridges the gap in existing literature by identifying emerging fraud threats driven by digital banking advancements and proposing innovative, technology-driven fraud prevention strategies tailored to Banc ABC's operational environment.

2.7.0 Conclusion

A review of existing literature reveals significant gaps in understanding fraud within Banc ABC's specific operational context. While prior research has broadly examined financial fraud across various sectors, it has not provided a detailed analysis of the unique fraud risks faced by Banc ABC or the effectiveness of its current fraud prevention strategies. This study addresses these gaps by contextualizing fraud prevention models within Banc ABC, applying financial intelligence principles tailored

to Zimbabwe's banking sector, and assessing their practical applicability. Additionally, it evaluates real-world fraud cases, investigates the bank's fraud detection mechanisms, and proposes targeted solutions based on empirical data. Furthermore, the study explores emerging fraud risks associated with digital banking advancements and recommends how Banc ABC can leverage artificial intelligence, blockchain, and advanced data analytics to enhance its fraud prevention framework. By bridging these theoretical and empirical gaps, this research contributes valuable insights to the field of financial intelligence and fraud prevention in Zimbabwe. The findings will serve as a resource for banking professionals, policymakers, and researchers, offering practical strategies for strengthening fraud risk management and ensuring regulatory compliance within Zimbabwe's banking industry.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction.

This chapter presents the methodology adopted for this research, detailing the approach used to collect, analyze, and interpret data regarding fraud detection and prevention in Banc ABC. The research methodology is critical as it determines the reliability and validity of findings. This chapter elaborates on the research design, population, sampling techniques, sources of data, research instruments, data collection procedures, and analysis methods employed in the study. Ethical considerations and reliability measures undertaken to ensure the credibility of the study are also discussed. The methodology selected aligns with the research objectives, providing a structured framework for investigating the effectiveness of fraud prevention mechanisms within Banc ABC.

3.1 Research Design

The research design serves as the blueprint for conducting the study, outlining the systematic plan for data collection, analysis, and interpretation. A well-defined research design ensures that the research questions are adequately addressed through appropriate methodologies. For this study, a descriptive research design was employed to provide a detailed analysis of fraud prevention strategies at Banc ABC. Descriptive research is appropriate for understanding the how and why of a phenomenon, making it suitable for exploring the effectiveness of internal control measures in detecting and preventing fraud.

A case study approach was also adopted to examine Banc ABC specifically. The case study methodology allowed for an in depth investigation into the bank’s fraud prevention strategies, drawing insights from real world occurrences and operational policies. Case study research is beneficial when exploring complex phenomena within their real-life context, making it particularly useful for analyzing financial fraud and

control systems. The selected design facilitated a thorough assessment of existing fraud detection mechanisms while identifying potential areas for improvement.

3.2 Descriptive Research Design

The study employed a descriptive research design, which is widely recognized for its effectiveness in analyzing contemporary issues through observation, documentation, and analysis of existing systems. Descriptive research aims to systematically describe a situation, problem, or phenomenon without manipulating variables. In this study, it was used to assess the effectiveness of Banc ABC' s fraud prevention measures.

A similar approach was used in a study by Silas Nyaga Micheni (2016), which focused on the effectiveness of internal controls in detecting and preventing fraud in commercial banks listed on the Nairobi Securities Exchange. Micheni's study sought to determine how internal control mechanisms enhance fraud prevention, making it comparable to this research. Given the similarities in objectives, the descriptive research design was deemed appropriate for evaluating Banc ABC's internal controls. This method allowed for a comprehensive understanding of fraud prevention measures and their applicability in a real-world bank context

3.3 Population

The target population consisted of employees from Banc ABC, specifically from departments responsible for fraud detection and financial oversight. These included:

Department	**Staff Members**
Finance	15
Cyber security unit	10
Risk Management	10
Internal Audit	10

Compliance	10

Table 3.1 Banc ABC target population

In total, all employees formed the population but according . These employees were deemed relevant due to their direct involvement in fraud monitoring, compliance enforcement, and internal control systems.

3.4 Sampling Techniques

A non-probability sampling technique was used in selecting participants for the study. Non-probability sampling is commonly employed in qualitative research, where participants are chosen based on specific characteristics rather than random selection. This method was selected because it allows for targeted data collection from individuals with direct knowledge of fraud prevention mechanisms within Banc ABC.

Purposive sampling, a subset of non-probability sampling, was applied to select respondents based on their expertise and involvement in fraud detection. Purposive sampling ensures that only knowledgeable participants contribute to the research, enhancing the validity of findings. Employees from the finance, risk management, and internal audit departments were selected to provide insights into the effectiveness of fraud detection measures.

A probability sampling approach was adopted for participant selection to enhance statistical generalizability (Cochran, 1977). This methodology ensures all eligible members of the target population have a calculable probability of selection, thereby minimizing selection bias and supporting population-level inferences (Kish, 1965). The approach was implemented to achieve proportional representation of all key departments involved in fraud oversight at Banc ABC.

Stratified random sampling a recognized probability method, was specifically employed (Lohr, 2019). Consistent with standard practice, the target population (Table 3.1) was partitioned into mutually exclusive strata based on departmental function: Finance, Cyber Security Unit, Risk Management, Internal Audit, and Compliance (Levy & Lemeshow, 2013). Simple random sampling was then administered within each stratum (Thompson, 2012). This design guaranteed proportional inclusion of all critical

functional units responsible for fraud detection, ensuring comprehensive perspective representation across the organization's control environment.

3.5 Sample Size

For the purpose of this study, the researcher adopted the Krejce and Morgan formula and with a targeted population of 55 respondents, Krejce and Morgan formula gave a sample of 48 respondents as indicated below:

Thus Krejcie & Morgan formular:

$$s = \frac{X^2 NP(1-P)}{d^2(N-1) + X^2 P(1-P)}$$

s = required sample size.

X^2 = the table value of chi-square for 1 degree of freedom at the desired confidence level (3.841).

N = the population size.

P = the population proportion (assumed to be 0.50 since this would provide the maximum sample size).

d = the degree of accuracy expressed as a proportion (0.05)

$$s = \frac{3.841(55)(0.5)(1-0.5)}{0.05^2(55-1) + 3.841(0.5)(1-0.5)}$$

$s = 48$

Table 3.2 Sample size

Method of Data Collection	**Number of Participants**
Questionnaires	38

Interviews	10
Total Sample Size	**48**

3.6 Sources of Data

The research relied primarily on primary data gathered directly from respondents using structured questionnaires and semi-structured interviews. These tools ensured that the information collected was specific, first hand, and relevant to the research objectives.

3.7 Research Instruments

This section outlines the research instruments that were employed to collect data for the study. The selection of appropriate instruments was guided by the research objectives and the need to obtain both quantitative and qualitative data to explore the role of financial intelligence in preventing fraudulent activities. As this study adopted a mixed-methods approach, the instruments included structured questionnaires for quantitative data collection and semi-structured interviews for qualitative insights. These tools were chosen for their reliability, practicality, and ability to capture diverse perspectives from personnel across different departments within BancABC. The following subsections describe these instruments in detail, including their structure, purpose, and relevance to the research questions.

3.7.1 Questionnaires

Structured questionnaires included both closed-ended questions for quantitative analysis and open-ended questions to gather deeper qualitative insights. This instrument allowed efficient data collection and enabled respondents to elaborate on their views and experiences.

3.7.2 Interview Guide

Semi-structured, face-to-face interviews were conducted using an interview guide as the primary research instrument. The guide included open-ended questions designed to explore key themes around fraud prevention, internal controls, and organizational challenges specific to Banc ABC.

These interviews targeted selected employees from the Finance and Compliance departments due to their direct involvement in fraud detection and policy enforcement. The semi-structured format allowed for flexibility in probing deeper into participants' responses, thus generating richer qualitative data and uncovering insights that may not have been captured through questionnaires alone.

The use of an interview guide ensured consistency across interviews while allowing the researcher to adapt to emerging themes, clarify responses, and explore complex issues in greater depth.

3.8 Validity and Reliability

To ensure validity, the research instruments were pre-tested on two non-sampled employees. This allowed for adjustments in question wording and sequence for clarity and relevance.

Reliability was ensured by standardizing data collection procedures. Interview and questionnaire responses were cross-verified for consistency, and common themes were identified to reinforce the reliability of findings.

3.9 Data Collection Procedures

The data collection process followed a clear and ethical sequence, beginning with the administration of questionnaires and followed by interviews. The study employed both quantitative and qualitative approaches, making it essential to carefully coordinate how data was gathered from respondents at Banc ABC.

The first stage involved distributing structured questionnaires, which were the primary tool for collecting quantitative data. After securing formal permission from Banc ABC's management to conduct the study, a list of employees from relevant departments Finance, Risk Management, Internal Audit, and Compliance was obtained. The researcher then contacted selected participants to brief them about the purpose of the study, the nature of the questions, and their rights as respondents. Consent was obtained from all participants before any instruments were administered. Questionnaires were distributed through two methods: some were emailed to participants who preferred digital access due to workload or location, while others were physically handed out to those available on-site. Each respondent was given adequate time ranging from one to

three working days to complete the forms. The completed questionnaires were collected in sealed envelopes to ensure confidentiality. The researcher reviewed responses for completeness and entered the data into SPSS for quantitative analysis.

The second stage involved conducting semi structured interviews to collect qualitative data and deepen the understanding of issues raised in the questionnaires. An interview guide was developed and used to maintain consistency across all interviews while still allowing flexibility for probing further where necessary. Interviews were held in private office spaces at Banc ABC to ensure confidentiality and minimize disruptions. Each session lasted between 20 to 30 minutes. The researcher personally conducted all interviews and, with the interviewee's permission, used a voice recorder to capture the conversation accurately. In addition to recording, the researcher also took handwritten notes to highlight key points and ensure backup documentation. This combination allowed for accurate transcription and rich thematic analysis later.m

Several challenges were encountered during data collection. One of the main difficulties was coordinating with busy professionals, many of whom had limited time due to work pressures. To overcome this, the researcher offered flexible scheduling, including conducting some interviews during lunch breaks or after working hours. Another challenge involved initial reluctance from a few participants who feared their responses might not remain anonymous. To address this, the researcher emphasized that no names or identifiable information would appear in the final report and explained how all responses would be coded and stored securely. Trust was built by maintaining transparency throughout the process and reaffirming the academic nature of the study.

Ethical principles were rigorously upheld throughout the data collection process. Participation was strictly voluntary, and each respondent had the right to withdraw at any point without penalty. The confidentiality of all data was maintained by anonymizing responses and storing digital files in encrypted, password-protected folders, while hard copies were kept in locked storage accessible only to the researcher. By maintaining ethical discipline and flexibility, the data collection process was successfully completed and yielded rich data for both quantitative and qualitative analysis.

3.10 Data Presentation and Analysis

The data collected in this study was analyzed using a mixed methods approach, combining both quantitative and qualitative techniques to ensure a comprehensive and multidimensional understanding of fraud prevention strategies at Banc ABC. This dual approach aligned with the study's methodology, which incorporated structured questionnaires for statistical analysis and semi structured interviews for thematic exploration.

For the quantitative aspect, data from the closed-ended questions in the questionnaires were systematically coded and entered into SPSS (Statistical Package for the Social Sciences). SPSS was chosen for its robust statistical capabilities, allowing for the generation of descriptive statistics such as frequencies, means, and percentages. These metrics helped to identify patterns and measure respondent opinions on key fraud prevention practices, internal controls, and compliance procedures. The data was analyzed in relation to demographic information, departmental representation, and specific fraud detection practices to ensure that findings were representative of the broader sample selected through statistically validated sampling.

On the qualitative side, data was obtained from open-ended questionnaire responses and transcripts of the face-to-face interviews conducted using an interview guide. A thematic analysis approach was applied to this data. The process involved familiarization with the data, coding recurring phrases or ideas, categorizing those codes into meaningful themes, and interpreting the significance of each theme in the context of Banc ABC s internal fraud risk environment. Themes such as lack of inter departmental coordination need for regular staff training and over-reliance on manual reporting systems emerged as critical areas for improvement. The analysis also helped to explain or elaborate on patterns observed in the quantitative data, thereby enriching the interpretation and validating the results.

To maintain transparency and clarity, the results were presented using a combination of visual aids including bar charts, pie charts, frequency tables, and thematic summary matrices. These visuals were carefully selected to illustrate key findings in an accessible format and to support the narrative explanations. For example, charts were used to show the distribution of responses on fraud detection effectiveness, while thematic tables

summarized qualitative patterns from interviews, such as concerns about technological limitations in fraud monitoring.

By integrating both quantitative and qualitative findings, this study ensured that the data analysis remained consistent with the sampling strategy, the instruments used (questionnaires and interview guides), and the data collection procedures described in earlier sections. Quantitative data provided the breadth needed to generalize patterns across the institution, while qualitative data offered depth and context by capturing individual insights and experiences. This comprehensive analytical approach enhanced the validity of the findings and provided a solid foundation for the recommendations presented in the next chapter.

3.11.0 Ethical Considerations.

Ethical considerations were paramount throughout the research process to ensure the integrity of the study and the protection of participants' rights. The following principles were strictly observed:

3.11.1 Informed Consent

All participants were fully informed about the nature, purpose, and scope of the research prior to their involvement. A written consent form was provided and explained to each respondent, outlining their rights, the voluntary nature of participation, and the intended use of the data collected. Only those who provided written consent were included in the study. This process ensured that participants willingly took part in the research with a clear understanding of what it entailed.

3.11.2 Confidentiality

To maintain the privacy of respondents, all data collected was treated with strict confidentiality. Participants' names, job titles, and any identifying information were excluded from the final report. Anonymized codes were used to represent respondents during analysis. Furthermore, any information that could indirectly reveal the identity of a participant or department was omitted from the presentation of results. Confidentiality was essential in building trust and encouraging honest, uninhibited responses.

3.11.3 Right to Withdraw

Participants were informed that their participation was completely voluntary and that they could withdraw from the study at any point without facing any negative consequences. This right was communicated both verbally and in writing. If a participant chose to withdraw, any data already collected from them would be excluded from the final analysis. Emphasizing this right helped foster a sense of autonomy and respect for individual choice.

3.11.4 Non Maleficence

The research was designed to avoid any form of harm physical, psychological, or emotional to the participants. The nature of the questions was non-intrusive, and interviews were conducted in a professional, respectful manner. Participants were assured that their responses would not be used against them in any way and that no information would be shared with their employer. The study was careful to uphold the principle of "do no harm" throughout the data collection and reporting phases.

3.11.5 Data Protection

All data collected during the research process was securely stored, both digitally and physically. Digital files were encrypted and stored on password-protected devices, while hard copies were kept in locked storage accessible only to the researcher. Data was used exclusively for academic purposes and in accordance with research ethics protocols. After the completion of the study, all personal data will be securely deleted or destroyed to prevent any unauthorized access or misuse.

3.11.6 Conclusion

This chapter outlined the methodological framework adopted for the research. By applying a descriptive case study design, purposive sampling, and mixed data collection instruments, the study ensured a structured and ethical approach to analyzing fraud prevention strategies at Banc ABC. The combination of SPSS-based quantitative analysis and qualitative thematic analysis enhanced the reliability and depth of findings, paving the way for informed recommendations in subsequent chapters.

CHAPTER IV

DATA ANALYSIS, INTERPRETATION AND PRESENTATIONS

4.0. Introduction.

This chapter provides a detailed summary of the study's findings, covering participant proportions, demographic profiles, reliability statistics, frequency distributions, graphical data presentations, and an analysis aligned with the research objectives. The data was analyzed using SPSS version 26, incorporating both descriptive and inferential statistical methods, alongside thematic analysis for qualitative insights.

4.1. Response Rate.

This section presents the response rate for the questionnaire and interview.

4.1.1. Questionnaire Response Rate.

The table below shows the questionnaire response rate.

Table 4.1 Questionnaire Response Rate

Variable	Questionnaire Distributed	Questionnaire Returned	Response Rate %
Number of Respondents	38	35	92.1%

Source: Primary Source [2025]

The data in Table 4.1 shows that out of 38 distributed questionnaires, 35 were completed and returned, resulting in a high response rate of 92.1%. This high response rate indicates strong participant engagement and interest in the subject matter, which enhances the reliability and validity of the findings. The return rate suggests that the study's sample is sufficiently representative and the results can be generalized to the target population of banking and financial sector personnel in Harare CBD.

4.1.2. Interview response Rate.

The table below shows the interview response rate.

Table 4.2 Interview Response Rate.

Variable	Scheduled Interviews	Conducted Interviews	Response Rate
Number of Respondents	10	8	80%

Source: Primary Source [2025]

Table 4.2 indicates that 10 interviews were scheduled, and 8 were successfully conducted, resulting in a response rate of 80%. This is considered a strong response rate for qualitative interviews, which often face logistical challenges such as scheduling conflicts or non-consent from potential participants. The 80% success rate suggests adequate representation of views from key informants within Banc ABC and ensures that rich, qualitative insights support the quantitative data collected through the questionnaire.

4.2 Demographic characteristics of respondents

4.2.1 Respondents' Gender

The researcher inquired about the gender characteristics of the participants to mitigate the potential for gender bias in the resulting data.

Table 4.3 Gender population

gender	frequency	Percentage%
male	20	57.1
female	15	42.9

Source: Research Data [2025]

Table 4.3 presents the gender composition of the study participants. Out of 35 respondents, 57.1% were male and 42.9% were female. This indicates a reasonably balanced gender representation, though males slightly outnumber females. This distribution reflects the gender dynamics typically observed in the banking and financial services sectors in Zimbabwe, where men historically occupy a higher number of positions, particularly in technical and leadership roles. The inclusion of a significant proportion of female respondents strengthens the validity of the research by reducing gender bias and promoting inclusivity in data interpretation.

4.2.2 Age of participants.

The table below shows the ages of respondents.

Table 4.4 Ages of participants.

Ages	Frequency	Percentage %
18 - 25	4	11.4
26 – 44	25	71.4
45 – 54	3	8.6
Above 54	3	8.6

Source: Research Data [2025]

Table 4.4 shows that the majority of respondents (71.4%) are aged between 26 and 44 years, indicating a relatively young and active workforce. This age group typically comprises mid-level professionals and emerging leaders in the financial services sector, making them ideal informants for a study. The presence of older age groups 45–54 (8.6%) and above 54 (8.6%) adds experienced perspectives, particularly regarding long-term trends in fraud patterns and institutional responses. The 18–25 group, at 11.4%, consisted of entry-level professionals and junior staff, whose responses offered fresh insights and perceptions regarding technology-driven fraud prevention systems.

4.2.3 Level of qualification.

The table below shows level of qualification.

Table 4.5 Level of qualification.

The level of academic qualifications.		
Qualification	Frequency	Percentage %
Post Graduate Degree	7	20
Undergraduate Degree	22	62.9
Higher Diploma	2	5.7
Other professional courses	4	11.4
Total Male	**35**	**100**

Source : Research Data [2025]

Table 4.5 reveals that the majority of respondents (62.9%) possess undergraduate degrees, while 20.0% have attained postgraduate qualifications. This high level of academic achievement indicates a workforce that is well-equipped to understand and interact with complex systems like Financial Intelligence (FI). The presence of respondents with certificates and diplomas (17.1%) also reflects inclusivity of mid-level technical professionals who often play hands-on roles in fraud detection and reporting processes. These results suggest that the respondents have the requisite academic background to comprehend financial crime schemes and contribute meaningfully to

fraud prevention strategies. The dominance of degree holders ensures the credibility and quality of the data collected.

4.2.4 Sector of Employment.

The table below shows all the respondents' sectors of employment.

Table 4.6 Sector of employment.

Sector of employment	Frequency	Percentage %
Cybersecurity unit	8	22.9
Finance	8	22.9
Risk management	8	22.9
Internal audit	5	14.3
Compliance department	6	17.1

Source : Research Data [2025]

The data shows that Cybersecurity, Finance, and Risk Management are the most represented departments, each contributing 22.9% of respondents. This balance among the three core units emphasizes their central role in detecting, reporting, and managing financial fraud risks at BancABC.Internal Audit (14.3%) and Compliance (17.1%) departments are also represented, though slightly less. These areas are traditionally tasked with ensuring operational integrity, adherence to regulatory frameworks, and assessing the robustness of internal control systems.

4.2.5 Work experience

The table below shows the work experience.

Table 4.7 Work experience.

Working experience		
Experience	**Frequency**	**Response %**
Less than 3 year	2	5.7
3 to 5 years	18	51.4
6 to 10 years	12	25.7
More than 10 years	33	17.1
Total	**35**	**100**

Source: Research Data [2025]

The majority of respondents (51.4%) have between 3 to 5 years of experience, suggesting that they are relatively early-to-mid-career professionals who have already

developed some expertise in the field but are still exposed to modern training and current fraud prevention systems. Respondents with 6 to 10 years of experience constitute 25.7%, while those with over 10 years of experience make up 17.1%. These two groups bring a seasoned perspective, likely understanding the evolution of financial intelligence mechanisms and fraud tactics over time. Only 5.7% of respondents have less than 3 years of experience, implying that the survey responses are not heavily skewed by novice opinions, which adds credibility to the results.

4.3. Types of Fraud Occurring at Banc ABC

The first objective of the study was to document types of fraudulent activities occurring at Banc ABC. The following table depict the common types of fraud occurring:

Table 4.8 Common types of fraudulent activities being experienced

Type of fraudulent activity	1		2		3		4		5		**Statistics**	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Mean **μ**	S.D **σ**
Cyber fraud	2	5.7	7	20	9	25.7	9	25.7	8	22.9	3.41	1.24
Bank fraud	4	11.4	7	20	14	40	5	14.3	5	14.3	2.99	1.17
electronic card fraud	7	20	5	14.3	6	17.1	9	25.7	8	22.9	3.16	1.44
Insurance fraud	5	14.3	5	14.3	6	17.1	11	31.4	8	22.9	3.34	1.39
Financial statement fraud	1	2.9	5	14.3	6	17.1	13	37.1	10	28.6	3.74	1.17
Identity theft	1	2.9	3	8.6	9	25.7	15	42.9	7	20	3.69	1.02
Investment fraud	0	0	3	8.6	8	22.9	13	37.1	11	31.4	3.91	0.98

Source : Research Data [2025] *N=35*

4.3.1 Cyber Fraud

Table 4.8 shows that card fraud was reported to occur “very frequently” by 22.9% of respondents, while 25.7% said it occurs “frequently” and another 25.7% said “sometimes”. Only 5.7% indicated it “never” occurs. This results in a mean score of 3.41 with a standard deviation of 1.24, indicating a generally high occurrence of cyber fraud, though with some variance in perception across departments. The relatively high percentage of frequent and very frequent responses is being attributed by the growing digitization of banking services and increased online customer interaction. This aligns with research by McKinsey (2023), which found that cyber-related threats have more than doubled for African banks following rapid fintech adoption.

One interviewee from the Mt Pleasant branch from bank's cybersecurity unit confirmed, *“We are constantly targeted by phishing emails and malware, especially around end-of-month salary processing periods”.*

4.3.2 Bank Fraud

Bank fraud includes embezzlement or manipulation of banking operations, scoring a mean of 2.99 and a standard deviation of 1.17. This suggests that while not as prevalent as cyber fraud, it still occurs with moderate frequency. Table 4.4 shows that 40% of respondents selected sometimes, while only 14.3% reported very frequently. This reduced frequency compared to cyber fraud is due to stronger internal controls and banking supervision mechanisms now in place.

One compliance officer from Msasa branch explained, *“Bank fraud has declined due to automation in approval chains and improved segregation of duties.”*

4.3.3 Electronic Card Fraud

Table 4.8 indicated that ATM skimming and card cloning had a mean score of 3.16 and a standard deviation of 1.44, suggesting moderate frequency but with considerable variability across respondents. A total of 25.7% indicated it occurs frequently, and another 22.9% said very frequently. Electronic card fraud, with its high standard deviation, implies that some departments, especially customer service, encounter it more than back-office units.

A finance manager noted, *“We've had reports from clients about cloned cards being used in online transactions. It tends to spike during holidays or promotions.”*

4.3.4 Insurance Fraud

Insurance fraud exhibited a relatively high frequency, with a mean of 3.34 and a standard deviation of 1.39. Around 31.4% said it occurs frequently and 22.9% selected very frequently. Respondents cited fraudulent claims and misrepresentation of personal or asset information.

Interview data with one internal auditor stating, *"People understate risk when applying, then overstate damage during claims. It's subtle, but it's fraud."*

4.3.5 Financial Statement Fraud

Financial statement fraud had a high mean of 3.74 and a relatively low standard deviation of 1.17, suggesting strong agreement among respondents that this type of fraud occurs frequently. 28.6% of participants said it occurs very frequently, and 37.1% selected frequently. This clearly shows potential weaknesses in internal governance, risk management, and audit oversight. The Association of Certified Fraud Examiners (ACFE) 2022 Global Fraud Study also identified financial statement manipulation as the highest form of occupational fraud globally.

One senior auditor shared, *"Some units manipulate revenue or loss reports to meet unrealistic performance expectations."*

4.3.6 Identity Theft

Identity Theft recorded a mean of 3.69 and the lowest standard deviation of all variables (1.02), showing that nearly all departments observe this fraud type with high frequency and consistent severity. 42.9% of respondents reported it occurs "frequently" and 20% said "very frequently." This uniformity suggests it is widespread and systemic.

One interviewee from IT noted, *"We've had several cases where customer accounts were accessed after credentials were compromised online." The increase in mobile and online banking may contribute to this trend, particularly if multi-factor authentication is not enforced."*

4.3.7 Investment Fraud

Table 4.8 shows 37.1% of respondents selected "frequently" and 31.4% said "very frequently," showing strong agreement across the board. Investment fraud was identified as the most frequent type of fraud, with a mean of 3.91 and a low standard deviation of 0.98. Interviewees pointed to Ponzi schemes and fake investment portfolios as key issues.

A compliance manager explained, *"Fraudsters are using fake documentation and impersonation to lure clients into fake high-yield investment opportunities, often under names that sound legitimate."*

4.4. Role of financial intelligence in fraud detection and prevention.

The following table 4.8 depicts the role of financial intelligence in fraud detection and prevention.

Table 4.9 Roles of Financial in fraud detection and prevention

Role of financial intelligence in fraud prevention	**1**		**2**		**3**		**4**		**Statistics**	
	Freq	%	Freq	%	Freq	%	Freq	%	Mean **μ**	S.D **σ**
FI plays a significant role in detecting fraud at Bank ABC.	0	0	0	0	17	48.6	18	51.4	3.51	0.51
Suspicious activity reporting (SARs) is effective in identifying fraud.	0	0	4	11.4	14	40	17	48.6	3.37	0.67
FI tools and systems are well integrated in daily operations.	2	5.7	3	8.6	16	45.7	14	40	3.20	0.84
Staff members are adequately trained in using FI systems.	5	14.3	6	17.1	13	37.1	11	31.4	2.86	1.04
FI promotes accountability and transparency within the bank.	0	0	0	0	10	28.6	25	71.4	3.71	0.45

Source : Research Data [2025] N=35

4.4.1 FI plays a significant role in detecting fraud at Bank ABC

Table 4.9 shows a total of 35 respondents agree that financial intelligence plays a significant role in detecting fraud. It received the highest support, with 51.4% strongly agreeing and 48.6% agreeing, yielding a mean of 3.51 and a low standard deviation of 0.51, indicating strong consensus. This suggests that FI mechanisms are seen as vital to the bank's anti-fraud strategy. This aligns with Mugarura (2020), who emphasizes that FI enhances early detection by analyzing transaction patterns and behaviors.

4.4.2 FI promotes accountability and transparency within the bank

Respondents indicated that FI promotes accountability and transparency within the banking sector, with 71.4% strongly agreeing and a mean score of 3.71 and a standard deviation 0.45. This reflects the perception that FI frameworks enforce traceability and reinforce ethical standards in financial institutions.

An interviewee, one compliance officer mentioned, "*Whenever Financial Intelligence processes are enforced correctly, there is little room for internal collusion because every step is logged."*

4.4.3 Suspicious Activity Reporting (SARs) is effective in identifying fraud

Table 4.9 indicated that respondents had some variation in perception about statement Suspicious Activity Reporting (SARs) as effective in identifying fraud, 48.6% strongly agreed, but 11.4% disagreed, suggesting inconsistencies in the implementation or understanding of SARs.

An internal auditor remarked, *"Some staff lack the confidence to identify what counts as a suspicious transaction, which weakens SARs effectiveness."*

A compliance officer interviewed noted, *"SARs are useful, but sometimes staff hesitate to report suspicious activities due to fear of repercussions or lack of training."*

4.4.4 Staff members are adequately trained in using FI systems

Findings from table 4.9 shows substantial variation in responses, with a mean of 2.86 and a relatively high standard deviation of 1.04. A total of 31.4% strongly agreed, 37.1% agreed, but 14.3% strongly disagreed. This suggests a knowledge gap or uneven access to training programs. One cybersecurity staff member said, *"We need more refresher courses. Some departments have not been trained since implementation began."*

Training disparities were repeatedly mentioned. Staff in non-technical departments often lacked sufficient exposure to FI processes. These findings confirmed with

research by Chikweche and Mapuranga (2022), who found that financial institutions in Southern Africa often face barriers like uneven training and resource limitations, despite recognizing FI's importance.

4.5 Challenges in the implementation of financial intelligence measures.

Please rate the challenges faced in trying to implement fraud detection strategies.

Table 4.10 Challenges faced in the implementation of measures.

Challenges Faced in the implementation of financial intelligence measures.	1		2		3		4		5		**Statistics**	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Mean **μ**	S.D **σ**
Lack of skilled personnel in FI systems	2	5.7	5	14.3	8	22.9	12	34.3	8	22.9	3.54	1.20
Limited integration of FI tools across departments	0	0	7	20	7	20	11	31.4	10	28.6	3.69	1.10
Insufficient training on SARs and reporting procedures	0	0	8	22.9	7	20	12	34.3	8	22.9	3.57	1.09
Resistance to change from traditional fraud detection practices	0	0	4	11.4	6	17.1	13	37.1	12	34.3	3.94	1.02
Inadequate technological infrastructure	0	0	0	0	0	0	11	31.4	24	68.6	4.69	0.47

Source: Research Data [2025] *N=35*

4.5.1 Inadequate technological infrastructure

Table 4.10 shows a combined 100% of participants rated this factor as either a major (31.4%) or critical (68.6%) challenge, with a mean score of 4.69 and a low standard deviation of 0.47, indicating strong consensus among respondents. This highlights a severe limitation in the availability or robustness of systems needed to support sophisticated FI operations. The studies concur with Mavengere and Chirisa's (2022) study, which emphasized that poor infrastructure remains a major bottleneck in digitizing compliance systems in Zimbabwean banks.

An IT respondent noted, *"Our systems are outdated and cannot handle advanced analytics or real-time integration. This limits our ability to act on red flags promptly."*

4.5.2 Resistance to change from traditional fraud detection methods

Notably, 34.3% of respondents rated resistance to change from traditional fraud detection methods it a critical challenge, while 37.1% marked it as a major one, suggesting widespread cultural inertia with a mean of 3.94 and standard deviation of 1.02. This resistance stems from a lack of exposure to advanced Financial Intelligence tools or fear of redundancy.

An interviewee from the compliance unit mentioned, *"Senior staff often prefer paper trails and manual reviews, they don't trust AI to catch everything."*

4.5.3 Limited integration of Financial Intelligence tools across departments

Table 4.10 shows that a total of 60% of respondents rated limited integration of financial intelligence tools across departments as either a major or critical issue. Findings from the study gave a mean score of 3.69 and a standard deviation of 1.10. This suggests division in how FI systems are deployed across units such as audit, risk, compliance, and finance.

A risk manager interviewed stated, *"We don't have one dashboard linking all departments. Each team works in isolation, which delays responses."*

4.5.4 Insufficient training on SARs and reporting procedures

Approximately 57.2% of respondents rated insufficient training on suspicious activity reports as a major or critical concern, with a mean of 3.57 and a standard deviation of 1.09. This mirrors earlier findings that suggested some staff lack updated training. The relatively high mean suggests that, although institutions may have systems in place,

staff lack the procedural knowledge to use them effectively. These findings reflect broader gaps in internal training programs and are consistent with the assertions of Makumbe & Maravanyika (2023), who documented the lack of structured AML training in Zimbabwe's financial sector.

This was supported in interviews, with a junior banker confessing, *"No one ever taught me how to file a SAR. I just report upwards and hope someone does it."*.

Another frontline banking officer reported, *"I only learned about SARs during a fraud case; we were never trained formally on how to report suspicious activities."*

4.5.5 Lack of skilled personnel in Financial Intelligence systems

Table 4.10 indicated a total of about 57.2% of respondents saw this as a major or critical challenge, with a mean of 3.54 and a standard deviation of 1.20, again revealing a significant concern with considerable variability in experiences across institutions. While some institutions may have invested in skilled staff, others remain highly constrained.

As one internal auditor noted, *"We do not have qualified forensic analysts. We often rely on manual reviews, which are inefficient."*

4.6 Recommendations on strategies used to prevent and reduce fraud.

The table below shows the effectiveness of the recommended strategies used to prevent fraud. Respondents were tasked to demonstrate how effective and efficient are the measures/strategies in preventing fraud

Table 4.11: Recommended strategies to detect and prevent fraud.

Fraud detection strategies	**1**		**2**		**3**		**4**		**5**		**Statistics**	
	Freq	%	Freq	%	Freq	%	Freq	%	Freq	%	Mean **μ**	S.D **σ**
Regular audits and risk assessments	0	0	0	0	8	22.9	16	45.7	11	31.4	4.09	0.71
Enhanced transaction monitoring systems	0	0	0	0	1	2.9	11	31.4	23	65.7	4.63	055
Improved staff training and	0	0	3	8.6	3	8.6	18	51.4	11	51.4	4.06	0.87

awareness on fraud risks												
Collaboration with FIU and regulatory bodies	0	0	0	0	5	14.3	12	34.3	18	51.4	4.37	0.73
Investment in advanced analytics and artificial intelligence	0	0	0	0	0	0	8	22.9	27	77.1	4.77	0.42

Source : Research Data [2025] *N=35*

4.6.1 Investment in advanced analytics and artificial intelligence

This strategy received the highest mean score of 4.77 and a low standard deviation of 0.42. An overwhelming 77.1% rated it as very effective, and 22.9% as effective, with no negative ratings at all. This reflects a strong consensus around the capabilities of AI and analytics to detect complex fraud schemes in real time. This finding is in line with studies by PwC (2022), which found that AI-powered fraud detection increased early detection rates by over 70% in major banks across Africa.

An interviewee from the IT department said, *"AI gives us pattern detection capabilities we didn't have before. We can now identify anomalies within seconds, unlike traditional methods."*

4.6.2 Enhanced transaction monitoring systems

The second most effective strategy was Enhancing transaction monitoring systems which gave a mean of 4.63 and SD of 0.55. A total 65.7% of the respondents rated it very effective, and 31.4% effective. These tools, such as real-time alerts and cross-account monitoring, are crucial for identifying unusual transaction patterns.

A risk manager interviewed remarked, *"Our transaction monitoring dashboard is now integrated with multiple systems. Alerts come in real-time, allowing us to freeze accounts before damage is done."*

4.6.3 Collaboration with FIU and regulatory bodies

The collaboration with FIU and regulatory bodies strategy scored a high mean of 4.37 and a standard deviation of 0.73, with 51.4% rating it very effective. This suggests strong recognition of the role external stakeholders play in enhancing fraud intelligence

through data sharing and legal support. A study by Chikweche and Mapuranga (2023) supported the finding and in their research, they emphasised the role of inter-agency collaboration in strengthening AML frameworks in Zimbabwe.

One compliance officer noted, *"FIU involvement is critical. They help trace offshore transactions that would be impossible to follow internally."*

4.6.4 Regular audits and risk assessments

Table 4.11 shows that most respondents (77.1%) rated regular audits and risk assessment strategy as effective or very effective. The strategy scored highly with a mean of 4.09 and SD of 0.71. While still widely trusted, its slightly lower mean suggests audits are often seen as periodic and reactive, rather than ongoing or preventive.

An internal auditor explained, *"While audits are essential, they're usually done quarterly or annually, meaning some fraud may have already occurred before detection."*

4.6.5 Improved staff training and awareness

Findings from table 4.11 indicate that training and awareness are an effective strategy to prevent fraudulent activities. Most respondents, 82.8% agreed that training is effective only 8.6% rated it less effective. This was supported by a mean of 4.06 and a standard deviation of 0.87, showing a slightly wider spread of opinion. A percentage of 8.6% indicated that training programs are not yet uniform across departments.

A senior banker interviewed shared, *"Some training sessions are basic and don't reflect emerging fraud methods. We need continuous, role-specific learning."*

4.7.1 Discussion of findings.

This section provides a brief interpretation of the study's main findings in relation to the research objectives. It highlights how financial intelligence is being used to prevent fraud and discusses key trends, challenges, and insights drawn from the data.

4.7.2Prevalence of Fraudulent Activities at Banc ABC

The study established that fraudulent activities are widespread within Banc ABC, with investment fraud, financial statement fraud, identity theft, and cyber fraud being the most common. Investment fraud had the highest frequency, as respondents reported frequent incidents involving fake investment schemes and impersonation. This was

closely followed by financial statement fraud, which reflected manipulation of financial records for personal or departmental gain.

Identity theft also emerged as a severe issue, as a significant portion of staff acknowledged cases of compromised customer accounts. Cyber fraud, though slightly lower in mean score, was still reported by the majority, particularly in departments dealing with online platforms. These results are consistent with global findings by McKinsey (2023) and the Association of Certified Fraud Examiners (2022), which emphasize the growing threat of technology-driven financial crimes. The patterns observed in this study reflect how digitization, coupled with internal control gaps, contributes to fraud vulnerability in Zimbabwe's banking environment.

4.7.3The Role of Financial Intelligence in Fraud Prevention

The study found overwhelming agreement among participants that financial intelligence plays a significant role in detecting and preventing fraud. Respondents strongly supported the idea that FI enhances accountability, transparency, and the effectiveness of fraud detection systems through mechanisms such as Suspicious Activity Reports (SARs). The use of FI tools in day to day operations was also rated positively. However, there was noticeable concern regarding staff preparedness. Although most employees acknowledged the value of FI, many expressed uncertainty about using FI systems effectively due to limited training.

This disparity points to a disconnect between the availability of tools and the technical capacity to use them efficiently. The findings align with literature by Mugarura (2020), who emphasized the role of FI in uncovering suspicious patterns and transaction anomalies, and Chikweche and Mapuranga (2022), who highlighted training gaps in Southern African banking institutions. These results suggest that while FI has strong theoretical and operational potential, its success depends heavily on human capital and system integration.

4.7.4Challenges in Implementing Financial Intelligence Measures

The research identified several major obstacles to the effective implementation of FI mechanisms at Banc ABC. The most critical among them was inadequate technological infrastructure, with respondents unanimously citing outdated systems as a barrier to timely data analysis and real time fraud detection. Resistance to change from traditional

fraud detection methods was also a significant challenge. Many senior employees reportedly preferred manual procedures and paper-based systems, fearing that reliance on automated tools could compromise judgment or lead to redundancy.

Other noted challenges included limited integration of FI tools across departments, insufficient training on SAR procedures, and a shortage of skilled personnel to manage advanced fraud detection technologies. These findings are echoed in studies by Mavengere and Chirisa (2022), who pointed out infrastructure-related bottlenecks, and Makumbe and Maravanyika (2023), who emphasized training deficiencies as major roadblocks in the successful use of financial intelligence. The challenges identified highlight the need for both technical and cultural transformation to support FI effectiveness in Zimbabwean banks.

4.7.5 Effectiveness of Recommended Fraud Prevention Strategies

Participants identified several effective strategies to improve fraud prevention efforts at Banc ABC. Investment in advanced analytics and artificial intelligence (AI) received the highest rating, with strong support for its ability to identify unusual patterns and detect complex fraud schemes. Enhanced transaction monitoring systems were also highly rated, with respondents acknowledging their value in generating real-time alerts. Collaboration with external regulatory bodies, such as the Financial Intelligence Unit (FIU), was seen as another critical strategy, enabling inter-agency coordination and access to broader data networks.

Regular audits and staff training were also recognized as important but were rated slightly lower, possibly due to their perceived reactive nature. The emphasis on AI and real-time monitoring reflects a shift in industry best practices, as confirmed by PwC (2022), which found that digital tools improve detection rates significantly. The findings suggest that future fraud prevention must prioritise technology, interdepartmental integration, and capacity building to address both internal and external threats.

4.7.6. Summary.

This chapter details the research findings comprehensively. Information was collected via questionnaires and aided by relevant interview questions. It covered the response

rate, for the role of financial intelligence in preventing fraudulent activities The next chapter will focus on recommendations, conclusions, and a summary.

CHAPTER V

SUMMARY OF THE STUDY, CONCLUSION AND RECOMMENDATION

5.0 Introduction

This chapter presents a synthesis of the research by outlining the summary of the study, summarising key findings, drawing final conclusions, and providing strategic recommendations based on the data presented in Chapter Four. The aim is to consolidate how financial intelligence (FI) contributes to fraud prevention and to suggest practical measures for improving its implementation within Zimbabwean financial institutions, particularly BancABC.

5.1.1 Summary of the Study

The study explored the role of financial intelligence in detecting and preventing fraudulent activities, using BancABC as a case study. The research aimed to evaluate the effectiveness of FI tools and mechanisms, examine the types of fraud encountered in the institution, and assess the challenges faced in implementing FI-based fraud prevention strategies.

A mixed methods approach was used, combining quantitative data from structured questionnaires and qualitative insights from interviews. Data analysis included descriptive and inferential statistics via SPSS, as well as thematic interpretation. The sample consisted of 35 questionnaire respondents and 8 interview participants drawn from various departments, including compliance, risk, finance, internal audit, and cybersecurity.

The study was guided by key objectives, including identifying prevalent types of fraud, evaluating the use of financial intelligence in fraud detection, and assessing the challenges and effectiveness of fraud prevention strategies.

5.1.2 Summary of Findings

The study established that BancABC experiences a wide range of fraud types, with investment fraud, financial statement fraud, identity theft, and cyber fraud being the most common. Investment fraud had the highest frequency, often involving impersonation and fake portfolios. Identity theft and financial statement manipulation were also widespread, suggesting systemic vulnerabilities within the bank’s controls and customer verification processes.

5.1.3 Role of Financial Intelligence in preventing fraudulent activities

There was strong consensus among respondents that financial intelligence plays a critical role in fraud prevention. Most participants agreed that FI tools, such as

Suspicious Activity Reports (SARs), transaction monitoring systems, and audit trails, enhance accountability, transparency, and early detection. However, some staff members reported limited confidence in using FI systems due to inadequate training, which weakens the full utility of these tools.

5.1.4 Challenges in Implementation financial intelligence measures in fraud prevention

The biggest obstacle identified was inadequate technological infrastructure, followed by resistance to change, poor system integration, and insufficient training on SAR procedures. These findings suggest that while the tools may be in place, their effectiveness is undermined by operational inefficiencies and human capital limitations.

5.1.5 Effectiveness of Recommended Strategies

Strategies such as investment in artificial intelligence, enhanced transaction monitoring, and collaboration with regulatory bodies were deemed the most effective. AI based fraud detection tools received the highest rating for their ability to detect patterns and generate real time alerts. Regular audits and staff training, although important, were considered slightly less effective due to their reactive nature and inconsistent execution.

5.1.6 Conclusion

The study concludes that financial intelligence is indispensable in modern banking fraud prevention. The adoption of FI tools significantly improves fraud detection by enabling the identification of suspicious activities, promoting data driven decision making, and enhancing transparency across departments.

However, the effectiveness of FI at BancABC is currently hindered by infrastructural deficiencies, lack of staff training, resistance to digital transformation, and weak departmental integration. These factors dilute the potential of financial intelligence and expose the institution to persistent fraud risks.

Therefore, the successful prevention of fraud is not only dependent on the availability of advanced systems but also on institutional culture, workforce preparedness, and strategic collaboration with external regulators such as the Financial Intelligence Unit (FIU).

5.2.0 Recommendations

The findings of this study underscore the importance of a well-structured financial intelligence framework in combating fraud within financial institutions, particularly in the context of BancABC. However, several gaps were identified that hinder the full realisation of FI's potential ranging from technological limitations to staff capacity and resistance to change. Effective fraud prevention requires not only the presence of sophisticated tools but also an enabling environment supported by skilled personnel, institutional integration, and regulatory cooperation. The recommendations below are designed to address these challenges and enhance the effectiveness of financial intelligence in preventing fraudulent activities.

5.2.1 Upgrade Technological Infrastructure

BancABC should invest in modern and scalable IT systems capable of supporting Realtime fraud detection, advanced analytics, and integrated reporting tools .Upgrading infrastructure is essential because outdated systems limit the effectiveness of financial intelligence tools and delay timely responses to suspicious activities.

5.2.2 Implement Artificial Intelligence and Data Analytics

The bank should adopt AI-powered fraud detection systems capable of identifying suspicious patterns automatically. This is important because manual systems often miss complex fraud schemes that AI can detect more accurately and quickly.

5.2.3 Strengthen Interdepartmental Integration

A unified fraud management platform should be established to link departments such as compliance, audit, and IT. Integration is crucial because fragmented systems create communication gaps and delay coordinated responses to fraud.

5.2.4 Standardise and Expand Training on FI Tools

BancABC should implement continuous, role-specific training programmes on FI systems and SAR procedures. This is necessary because uneven staff knowledge reduces the overall effectiveness of fraud detection and reporting.

5.2.5 Promote a Culture of Compliance and Innovation

Management should foster an institutional culture that values accountability, ethics, and innovation in fraud prevention. Promoting such a culture is vital as resistance to change was a key barrier to implementing new FI measures.

5.2.6 Enhance Collaboration with External Regulatory Bodies

The bank should strengthen partnerships with the FIU and other regulatory authorities to support cross-border fraud investigations. Collaboration is essential because some fraud schemes extend beyond the bank's internal capacity to monitor and resolve.

5.2.7Conduct Frequent and Risk-Based Audits

BancABC should adopt continuous and risk-based auditing practices supported by data analytics. Regular and targeted audits are important as they help uncover hidden vulnerabilities before they are exploited by fraudsters.

REFERENCE

African Development Bank. (2023). Illicit Financial Flows in Africa. Available at: https://www.afdb.org.

Ahmed, A. (2021). Global Financial Governance and FIUs. Journal of Financial Regulation.

Albrecht, W.S., & Zimbelman, M.F. (2019). Opportunity factors in financial fraud. Fraud Examination (6th ed.).

American Bankers Association. (2023). SAR Training Effectiveness Report.

Anderson, R. (2001). Cyber Fraud Exploitation. Security Engineering: A Guide to Building Dependable Distributed Systems.

Association of Certified Fraud Examiners (ACFE). (2022). Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse. Available at: https://www.acfe.com/report-to-the-nations/2022

BancABC. (2022). Annual Fraud Report 2022. Harare: BancABC. Unpublished internal report.

Becker, G.S. (1968). Economic Deterrence Theory. Crime and Punishment: An Economic Approach.

Benson, M.L., & Simpson, S.S. (2020). White-Collar Crime: An Opportunity Perspective.

BioCatch. (2023). Global Fraud Threat Report.

Bologna, G.J., & Schwarz, R.J. (2015). Fraud Auditing and Forensic Accounting.

Chikweche, T., & Mapuranga, M. (2022). Training Gaps in Southern African Banking Institutions. Journal of Financial Compliance.

Chikweche, T., & Mapuranga, M. (2023). Inter-agency Collaboration in AML Frameworks. Southern African Banking Review.

CISA (Cybersecurity and Infrastructure Security Agency). (2022). Data Breach Analysis Report.

Cohen, L.E., & Felson, M. (1979). Routine Activity Theory. Social Change and Crime Rate Trends.

Cochran, W.G. (1977). Sampling Techniques (3rd .).

Cybersecurity Ventures. (2023). Cybercrime Damages Report 2023. Available at: https://cybersecurityventures.com/cybercrime-damages-2023.

Deloitte. (2025). Integrated Fraud Risk Management Report.

DiMaggio, P.J., & Powell, W.W. (1983). Institutional Theory. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality.

Dyck, A., et al. (2020). Whistle blowers and Fraud Detection. Journal of Accounting Research.

Egmont Group. (2013). FIU Operational Standards.

Egmont Group. (2022). AI-Driven Fraud Detection Report.

Egmont Group. (2023). Cross-Border Fraud Collaboration Report.

FATF (Financial Action Task Force). (2012). FIU Functions and Responsibilities.

FATF (Financial Action Task Force). (2020). Guidance on Financial Intelligence Units (FIUs). Paris: FATF. Available at: https://www.fatf-gafi.org/publications/financialintelligence/documents/guidance-fius .

FATF (Financial Action Task Force). (2022). Compliance and Regulatory Frameworks Report.

FATF (Financial Action Task Force). (2023) Global Trends in Financial Crime and Fraud. Paris: FATF. Available at https://www.fatf-gafi.org/publications/fatfgeneral/documents/global-trends-financial-crime-2023

FBI (Federal Bureau of Investigation). (2023). Internet Crime Report.

Gou, X. (2020). Financial Intelligence and Fraud Detection. New York: Springer.

IBM. (2023). Ransomware Threat Landscape Report.

IMF (International Monetary Fund). (2023). Financial Intelligence Systems and Economic Stability Report.

Interpol. (2023). Global Financial Crime Trends.

Jofre, S., & Gerlach, J. (2018). Forensic Data Analytics in FI. Journal of Financial Forensics.

Johnson, R., & Gibbs, P. (2019). FI Tools and Fraud Reduction. Journal of Financial Security.

Khan, S., Ali, M., & Rahman, A. (2022). Artificial Intelligence and Big Data in Fraud Detection. International Journal of Advanced Computer Science.

Kim, Y., & Bae, S. (2018). Suspicious Activity Identification. Journal of Financial Compliance.

Kim, Y., & Bae, S. (2022). Technology-Driven Fraud Opportunity Reduction. Computers & Security.

Kim, S., Park, J., & Lee, H. (2022). Innovations in AI-Driven Fraud Detection in the Banking Sector. Journal of Banking Technology.

Kish, L. (1965). Survey Sampling.

Kobets, M. (2024). The Protection of Businesses from Cyber Fraud, Including Phishing Attacks. Cybersecurity Journal.

Korotkaia, E., & Zvinoveva, O. (2024). Financial Fraud Types and Methods of Detection and Prevention. Journal of Financial Crime.

KPMG. (2023). Fraud and Financial Crime in Zimbabwe: Trends and Challenges. Harare: KPMG Zimbabwe. Unpublished internal report.

Kumari, P. (2022). Revenue Recognition Fraud. Accounting Review.

Levi, M. (2023). Proactive Financial Intelligence. Journal of Money Laundering Control.

Lohr, S.L. (2019). Sampling: Design and Analysis.

Lovel, H., & Bhagat, R. (2024). Artificial Intelligence Challenges and Its Impact on the Detection and Prevention of Financial Statement Fraud. Journal of Forensic Accounting.

Makumbe, T., & Maravanyika, D. (2023). AML Training Deficiencies in Zimbabwe. Southern African Banking Review.

Mamari, S., & Zadjali, M. (2024). Fraud in Insurance and the Application of Artificial Intelligence (AI) in Preventing Fraud. Insurance Fraud Journal.

Mavengere, K., & Chirisa, I. (2022). Infrastructure Bottlenecks in Digital Compliance. Zimbabwe Journal of Technology.

McKinsey & Company. (2023). Digital Banking and Fraud Trends in Africa Report.

Miller, T., & Zhang, L. (2021). Game Theory in Fraud Prevention. Journal of Economic Dynamics.

Mishra, P., & Singh, R. (2022). Collaboration in FI Systems. Financial Information Review.

Mohammed, A., & Rahman, H. (2024). Human Capital in FI Systems. Journal of Financial Intelligence.

Moore, J., & Dempsey, R. (2021). Capability Factors in Fraud. Journal of Business Ethics.

Mugarura, N. (2020). FI in Early Fraud Detection. Journal of Money Laundering Control.

Mugarura, N. (2021). Institutional Pressures for FI. Global Journal of Comparative Law.

Mutanda, A., & Maireva, T. (2023). The Effectiveness of Cyber Fraud Risk Management Strategies Adopted by Commercial Banks in Zimbabwe. Zimbabwe Banking Review.

Nagin, D.S. (2013). Deterrence in the Twenty-First Century. Crime and Justice.

National Insurance Crime Bureau. (2023). Insurance Fraud Statistics Report.

Ngai, E.W.T., et al. (2022). Game-Theoretic Models in Fraud Detection. Decision Support Systems.

NIST (National Institute of Standards and Technology). (2023). Card Fraud Trends Report.

OECD (Organisation for Economic Co-operation and Development). (2009). International FIU Collaboration.

OECD (Organisation for Economic Co-operation and Development). (2021). FI and Regulatory Compliance Report.

Power, M. (2023). Institutional Isomorphism and Fraud Risks. Journal of Financial Crime.

PwC (PricewaterhouseCoopers). (2022). AI-Powered Fraud Detection in African Banks Report.

Reurink, A. (2018). FI Analysis Techniques. Journal of Financial Crime.

Reserve Bank of Zimbabwe (RBZ). (2018). Annual Report on Banking Sector Fraud. Harare: RBZ. Unpublished internal report.

Reserve Bank of Zimbabwe (RBZ). (2022). Fraud and Risk Management in the Banking Sector. Harare: RBZ. Unpublished internal report.

Reserve Bank of Zimbabwe (RBZ). (2023). Digital Banking and Cybersecurity Report. Harare: RBZ. Unpublished internal report.

Sanction Scanner. (2025). Resistance to Technological Innovation in FI Report.

Scott, W.R. (2014). Institutional Theory. Institutions and Organizations.

Sharma, A. (2021). Social Engineering Tactics. Journal of Cybersecurity.

Sharma, R., & Chandel, J. (2021). Financial Statement Manipulation. Accounting Horizons.

Sharma, V., Chen, K., & Sheth, J. (2021). Electronic Card Fraud. Journal of Payment Systems.

Silas Nyaga Micheni. (2016). Effectiveness of Internal Controls in Detecting and Preventing Fraud in Commercial Banks. Nairobi Securities Exchange Study.

Smith, J. (2021). Compliance and Risk Management in Financial Institutions. London: Routledge.

Smith, T. (2023). FIUs in Global Security. International Journal of Financial Intelligence.

Taylor, R., & Evans, S. (2023). Financial Security Through Advanced Data Analytics and Fraud Detection Tools. Journal of Banking Security.

U.S. Securities and Exchange Commission. (2023). Investment Fraud Advisory.

UNODC (United Nations Office on Drugs and Crime). (2010). FIU Functions Handbook.

UNODC (United Nations Office on Drugs and Crime). (2023). Routine Activity Theory in FI Report.

Van Rooij, M., et al. (2020). Financial Literacy and FI Skills. Journal of Consumer Affairs.

Verizon. (2022). Data Breach Investigations Report.

Verma, P., & Gupta, S. (2024). The Application of Artificial Intelligence in Preventing Insurance Fraud. Journal of Insurance Technology.

Wolfe, D.T., & Hermanson, D.R. (2004). The Fraud Diamond. CPA Journal.

World Bank. (2022). FIU Operational Frameworks Report.

World Bank. (2023). FI and Economic Security Report.

ZACC (Zimbabwe Anti-Corruption Commission). (2021). Case Study: BancABC Insider Fraud. Harare: ZACC. Unpublished internal report.

ZCSA (Zimbabwe Cyber Security Agency). (2023). Phishing Campaigns in Zimbabwean Banks. Harare: ZCSA. Unpublished internal report.

Zhou, L. (2021). Expense Fraud Schemes. Journal of Forensic Accounting.

Zimbabwe Independent. (2021). Collapse of Ponzi Scheme in Harare. Available at: https://www.theindependent.co.zw

APPENDICIES

APPENDIX 1: RESEARCH ASSISTANCE LETTER

Bindura University of Science Education

P. Bag 1020

Bindura

Zimbabwe

To whom it may concern.

RE: REQUEST FOR RESEARCH ASSISTANCE.

I am Kudzaishe Brendon Jera, an undergraduate student at Bindura University of Science Education. I am studying for a Bachelor of Commerce (Honours) Degree in Financial Intelligence. As part of my studies, I am conducting a research study titled **The role of financial intelligence in preventing fraudulent activities: A Case study of Banc ABC Harare**

I would be tremendously grateful for your willingness to take part in this endeavour by providing an overview of the dangers posed by Fraudulent activities in banking system taking place . Please help me out by filling out the accompanying questionnaire.

It is completely up to you whether or not you participate in this survey, and you are authorized to do so without experiencing any penalties, at any moment. Also, you are informed that participating in the study will not provide you with any financial or other benefits.

I assure that the data gathered will only be utilized for this project as well as being handled with the highest level of confidentiality.

Yours Faithfully
Kudzaishe Jera

APPENDIX 2: QUESTIONNAIRE FOR BANC ABC STAFF

Section A: Demographic Information

1. Age Group: □ 20–30 years □ 31–40 years □ 41–50 years □ 51+ years

2. Gender: □ Male □ Female □ Prefer not to say

3. Department: □ Finance □ Risk Management □ Compliance □ Internal Audit □ Other (please specify): _____

4. Position in the Organization: □ Employee □ Manager □ Auditor □ Fraud Prevention Officer □ Other

5. Years of Service: □ Less than 2 years □ 2–5 years □ 6–10 years □ Over 10 years

Section B: What are prevalence and nature of at Banc ABC

6**. What types of fraud are most common at BancABC? (Check all that apply**)

□ Cyber fraud

□ Bank fraud

□ Electronic card fraud

□ Insurance Fraud

□Identity Fraud

□ Financial statement fraud

□Investment Fraud

□ Other (please specify): _____

Section C : Role of Financial intelligence in preventing fraudulent activities

Tick the box that best shows how much you agree with each statement

Use the same scale of 1-5

1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

Roles Financial intelligence	**1**	**2**	**3**	**4**	**5**
Financial Intelligence plays a major role in detecting fraud.					
Suspicious activity reporting (SARs) is					

effective in identifying fraud					
FI tools and systems are well integrated in daily operations.					
Staff members are adequately trained in using FI systems.					
FI promotes accountability and transparency within the bank.					

Section D: Challenges in Implementing Financial Intelligence Measures

1 **Please rate the following challenges using the same scale (1 = Strongly Disagree to 5 = Strongly Agree**

Challenges face in implementing Financial intelligence measures	**1**	**2**	**3**	**4**	**5**
Lack of skilled personnel in FI systems					
Limited integration of FI tools across departments					
Insufficient training on SARs and reporting procedures					
Resistance to change from traditional					

fraud detection practices					
Inadequate technological infrastructure					

Section E: Evaluation of Fraud Prevention Strategies

1 **Please rate the effectiveness of the following strategies (1 = Not Effective at All, 5 = Very Effective)**

Fraud detection strategies	**1**	**2**	**3**	**4**	**5**
Regular audits and risk assessments					
Enhanced transaction monitoring systems					
Improved staff training and awareness on fraud risks					
Collaboration with FIU and regulatory bodies					

Investment in advanced analytics and artificial intelligence					

APPENDIX 3: INTERVIEW GUIDE

1. What types of fraud are most commonly experienced at BancABC?

2. In your view, how effective is Financial Intelligence in detecting fraud at BancABC?
3. What role do Suspicious Activity Reports (SARs) play in identifying fraud?
4. Are staff members adequately trained in using FI tools such as SARs?

5. What challenges do you face when using Financial Intelligence systems at BancABC?
6. Why do you think there is resistance to moving from traditional methods to automated FI tools?
7. How well integrated are FI tools across departments like Risk, Compliance, and Audit?
8. Does the current technological infrastructure support effective FI operations?
9. What level of support does top management provide to FI-based fraud prevention efforts?
10. What recommendations would you suggest to improve FI-based fraud detection and prevention at BancABC?

APPENDIX 4: TURNITIN REPORT

kudzaishe jera.docx

ORIGINALITY REPORT

13%	10%	6%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.igi-global.com Internet Source	1%
2	Submitted to Midlands State University Student Paper	1%
3	www.coursehero.com Internet Source	<1%
4	ir-library.ku.ac.ke Internet Source	<1%
5	mis.itmuniversity.ac.in Internet Source	<1%
6	financialcrimeacademy.org Internet Source	<1%
7	ir.msu.ac.zw:8080 Internet Source	<1%
8	library.mua.ac.ke Internet Source	<1%
9	ulspace.ul.ac.za Internet Source	<1%
10	sumsub.com Internet Source	<1%
11	Adeniyi, Elizabeth O.. "Occupational Fraud: A Quantitative Study on the Impact of Enhancing Anti-Fraud Controls With Forensic Accounting", South College, 2025 Publication	<1%