Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

Enhancing Financial Crime Detection through Forensic Accounting Techniques in Zimbabwean Commercial Banks: A Critical Review and Integrated Investigative Framework

Tafadzwa Jimu[1*], Rumbidzai Chipindu[2], Liberty Magwizi[3]

[1*]Department of Finance and Accounting, University of Zimbabwe

[2]Department of Accounting Sciences, Midlands state university

[3]Department of Accounting Sciences, Midlands state university

Abstract

Purpose Commercial banks remain exposed to diverse forms of financial crime including money laundering, cyber financial crime, inside fraud, procurement fraud, unauthorized electronic money transfers, fraudulent financial statements and the disguise of movement of assets. The swift development of digital banking and economic instability in Zimbabwe has amplified the institutional exposure to financial crime. The research analyses the application of forensic accounting in enhancing financial crime detection and investigating capacity to improve fraud governance in Zimbabwean commercial banks.

Design/methodology/approach The research employed a conceptual and empirical literature review approach. Secondary data was gathered through the examination of journal articles, institutional reports, banking fraud articles, governance literature and forensic accounting literature. Thematic analytical synthesis approach was employed in discovering themes, conceptual links and institutional issues in relation to forensic accounting techniques and financial crime detection.

Findings Trace of transactions, digital forensic accounting, fraud analysis, forensic statement analysis, forensic interviewing, preservation of evidence, and financial reconstruction appeared to be crucial instruments in enhancing investigations into banking fraud. On the contrary, poor institutionalization of forensic accounting is the key obstacle facing the commercial banks in Zimbabwe.

Practical implications The research recommended that commercial banks should institutionalize forensic accounting units, improve fraud analytics mechanisms, enhance digital investigative capability and incorporate forensic evidential mechanisms into governance and compliance mechanisms.

Originality/value This article enriches the literature on forensic accounting and banking governance by presenting a new Forensic Accounting Investigative Framework-an Integrated Forensic Accounting Investigative Framework designed for Zimbabwean commercial banks and other emerging economies.

Keywords: Forensic Accounting, Financial crime detection, fraud investigation, commercial banks. Digital forensics, Governance.

1. Introduction

Financial crime is currently one of the most serious governance, operational and institutional threats facing banking systems in the world. Banks act as a central agent for financial intermediation, liquidity mobilization, capital flows, settlement of payments and financial growth and this critical position in national and global economies places them at the heart of money laundering, corruption, cyber-crime, insider dealing, procurement fraud, illicit finance, and financial statement falsification and ultimately compromises institutional credibility, public trust and macroeconomic stability (Levi and Reuter, 2006; Rezaee and Riley, 2019; Kassem and Higson, 2021). Occupational fraud remains one of the most pervasive and costliest forms of economic crime globally. The Association of Certified Fraud Examiners (ACFE) report stated that among the industries that suffer most from fraud, the financial sector remains vulnerable because of the huge number of transactions processed, high financial value involved and dependence on technology (ACFE, 2022).

Digitization has brought about rapid transformation in banking system thereby increasing both the magnitude and nature of financial crime. Online banking, mobile payment system, fin-tech integration, artificial intelligence transactions, automated clearing system and digital loan platform enhance operational efficiency and improve financial inclusion (Arner et al., 2020; Ozili, 2020; Mhlanga, 2024), however it equally provides opportunity for more cyber-financial fraud, phishing, ransomware, identity theft, fraudulent transactions, and digitally hidden assets, and manipulations of transactions (Broadhurst et al., 2020; PwC, 2022; FATF, 2023). Broadhurst et al. (2020) have opined that cyber-enabled financial crime is increasingly transnational in nature and highly sophisticated hence pose enormous challenge to conventional audit detection method.

Traditionally, financial auditing has been at the core of financial accountability and fraud prevention with internal and external audit systems, compliance functions and regulatory examinations, strengthening the integrity of reporting and verification of internal control mechanism (Messier et al., 2017; Hayes et al., 2020; Knechel and Salterio, 2016). Conventional auditing method is now being argued as not adequate to trace complex collusion, layered transactions, shell companies, digital manipulation and hidden ownership (Singleton and Singleton, 2010; Rezaee and Wang, 2019; Vona, 2020) as it mostly aims at assuring financial statement reliability and accuracy, while sophisticated financial crime requires evidence-based tracing and investigative approach (Rezaee and Riley, 2019).

This limitation further necessitated the rise in the importance of forensic accounting. Forensic accounting has become a unique discipline integrating the field of accounting, investigational analysis, interpretation of evidence, legal support, fraud detection and financial reconstruction (Hopwood et al., 2012; Bologna and Lindquist, 1995; Crumbley et al., 2017). Forensic accounting unlike conventional audit is designed for the examination of suspect transactions, computation of loss, tracking of asset, preservation of evidence, support of litigation, etc. According to Kassem and Higson (2021) forensic accounting has become a core part of fraud governance because modern financial crime often requires analysis and investigative work across different disciplines. Akinbowale et al. (2020) also stated that forensic accounting can improve transparency and accountability and enhancing financial resilience in banks.

As such, banks are an ideal target for fraud as financial crime generally involves the mix of technical cunning and behavioural or governance failures. Examples of commercial bank fraud are, but are not limited to, loan fraud with insider abuse, unauthorised withdrawals, irregular purchasing procedures, suspect related party transactions, money laundering, computer fraud, online fraud and intentional false accounting (Levi and Reuter, 2006; Manning, 2019; FATF, 2023). These types of activities are often found where there is weak controls, no division of duty, information asymmetry between top management and subordinates, collusion amongst insiders and diffuse ownership/control (Jensen and Meckling, 1976; Murphy and Free, 2021; Njanike and Mashayanye, 2023). Hence, the application and adoption of forensic accounting techniques have become paramount in an effort to address this trend and develop a more resilient banking system.

The application of several forensic accounting techniques is widely used in financial crime investigations nowadays. Transaction tracing assist investigators to trace criminal financial transaction, identifying

interrelationship between parties and uncover hidden money laundering channels (Manning, 2019; FATF, 2023). Digital forensic accounting enables the investigation of cyber fraud by adapting forensic accounting principles to investigate data such as meta-data, computer log, electronic foot-print, tampered computer system etc (Albrechtsen, 2020; Broadhurst et al., 2020). The role of financial statements in identifying fraud enables fraud detection through unknown liability, abnormal accounting method, overvalued asset and falsified reports (Rezaee and Wang, 2019; Vona, 2020). Fraud analytics can also facilitate the advancement of predictive fraud detection in identifying unusual behaviour, transactions and patterns (Bhasin, 2022; Kassem and Higson, 2021).

Financial crime is a significant developmental and governance issue in Africa. It is not an issue that the continent is overcoming, given that the flow of illicit financial activities, corruption, the failure of effective regulation and institutionality and the limitations in anti-fraud capability are present and eroding the financial system in most economies in the continent (UNECA, 2020; FATF, 2023; World Bank, 2023). Focusing on financial institutions, Akinbowale et al. (2020) demonstrate the ability of forensic accounting in bolstering fraud prevention, internal accountability and institutional integrity. Apart from the above, Bhasin (2022) opines that the developing countries must successfully institutionalize forensic accounting in a better way since the normal control mechanisms present in the accounting systems are no more equipped with handling modern day financial fraud.

The context of the forensic accounting for commercial banks will be well exemplified using Zimbabwe. The banking industry in Zimbabwe has experienced a high level of digital transformation for the past ten years by adopting mobile banking, internet banking, EFT and real-time gross settlement (RTGS) (Reserve Bank of Zimbabwe, 2023; Mhlanga, 2024).Despite financial inclusion and efficiency that arise from these technologies, the threat of cyber-financial crimes, fraudulent transactions (unexplained, anonymous and other transactions), identity fraud and illegal transfers, however, intensified (PwC, 2022; Mhlanga, 2024), making evidence-based forensic accounting systems more imperative. Macroeconomic instability further exacerbates fraud governance in Zimbabwe. High fluctuations in exchange rate, high inflation rates, lack of adequate liquidity, poor governance and institutions have created increased incentives for financial crimes while poor governance reduces monitoring capacity (World Bank, 2023; IMF, 2024; Njanike and Mashayanye, 2023). Banking-sector fraud is, therefore, more pronounced due to inadequate governance, ineffective internal controls and fragmented monitoring mechanisms (Njanike and Mashayanye, 2023). Therefore, Forensic accounting becomes not only an investigative but also a governance imperative.

The academic literature is abundant, however, lacks a substantial gap. The majority of the forensic accounting studies reviewed were concerned with the fraud prevention, auditing, anti-money laundering systems or corporate governance as whole. Very few critically assessed how the integration of forensic accounting methods would enhance detection of financial crime in the banking institutions of Zimbabwe. Typically, studies often critically assess the investigative capacity and the utilization of digital forensics, fraud analytics or auditing methodologies without constructing a composite investigative approach to cope with the changing banking nature.

This study seeks to bridge this research gap by critically reviewing how forensic accounting methods enhance the detection of financial crime in Zimbabwean commercial banks. The research uses the evidence-based review, theory triangulation and institutional review approaches to develop an Integrated Forensic Accounting Investigative Framework that relates fraud exposure, investigative accounting methods, governance inclusion and the institutional outcome.

2. Literature Review

The increasingly advanced nature of financial crimes has revolutionized the involvement of forensic accounting in banking governance, combating fraud and reinforcing corporate integrity. Originally, traditional accounting system was mainly focused on reporting the financial position and performance of a bank, validating transactions and confirming that standards are complied with. However, modern financial crimes involve more complex concealment strategies, such as manipulating the data through digital means, employing intricate schemes of layering the transactions, conspiring and colluding among employees/insiders, cyber-financial fraud, and so on, which would render traditional accounting and audit methods ineffective (Singleton and Singleton, 2010; Rezaee

and Riley, 2019; Vona, 2020). Hence, forensic accounting is established as a new, multidisciplinary field of investigation. Forensic accounting brings together expertise from accounting, law, auditing, criminal behaviour, governance, computer forensics and so forth (Crumbley et al., 2017). It's argued by Crumbley et al (2017) that forensic accounting is no longer about helping legal proceedings but increasingly used as a strategic governance instrument for the identification and prosecution of fraud, investigation of money laundering and tracing assets and for institutional transparency. By the same token, Kassem and Higson (2021) suggest that forensic accounting is gaining importance within anti-financial crimes system due to the increased technological sophistication of fraud and behavioural concealment.

A central discussion point in forensic accounting literature revolves around whether or not traditional auditing is still adequate enough to prevent financial crime, or if forensic accounting needs to exist as a standalone institutional framework to help detect, prevent, and prosecute financial fraud. Conventional audits are generally set to provide a reasonable assurance of financial statements, analyze internal control systems, and assist in a regulatory oversight function (Messier et al., 2017; Hayes et al., 2020; Knechel and Salterio, 2016). However, critics argue that auditing is essentially an assurance function, not a forensic investigative function, where auditors will generally look for the occurrence of material misstatements rather than focus on the complex financial manipulations typically utilized to conceal a fraud, which now involve collusion, shell corporations, unrelated parties, and other complex techniques (Rezaee and Wang, 2019). In addition, auditors will commonly find anomalies but typically will not delve deeply into reconstructing criminal financial activity, unlike a forensic accountant (Vona, 2020). Forensic accountants are said to have greater abilities to evidence and interpret behaviour, reconstruct finances, and ultimately develop stronger evidence specifically related to criminal activity within industries that have higher instances of criminal fraud, such as within banking institutions (Hopwood et al., 2012; Bologna and Lindquist, 1995; Kassem and Higson, 2021). The argument shows that forensic accounting is not intended to replace auditors, but should exist as a supporting and complementary institution for fraud governance.

In most of the forensic accounting procedures detailed in literature transaction tracing should be considered mostly in the context of AML and banking investigations. In relation to money laundering, transaction tracing can help recreate suspicious cash streams, reveal hidden transaction flows, lay open layering, and reveal any hidden relationships between accounts, subjects or beneficiaries (Manning, 2019; FATF, 2023). In criminal investigations criminals will typically disburse the proceeds of their crimes in various ways to disguise the origin of those criminal funds. Transaction tracing increases the ability of investigators to uncover money laundering networks, hidden transaction flows and suspicious financial relationships (Manning, 2019). The FATF states that transaction tracing continues to be important in preventing cross-border money laundering, hidden beneficial ownership and financial networks (FATF, 2023). In the banking system, analysis is vital in enabling transparency in to undetected fraud due to high volume transactions

Digital forensic accounting is another such crucial and significant tool which has gained rapid prominence ever since banking has been digitised. Examining electronic evidence such as metadata, digital logs, transactional timestamp, electronic mails and email trails, access logs, system trail of evidence, digitally altered documents etc. Are the key components of the process (Albrechtsen, 2020; Broadhurst et al., 2020; Chalu, 2022). Since cyber-financial fraud is being conducted increasingly in an international and complex way, the need for digital forensic capability to counter financial fraud has been identified (Broadhurst et al., 2020). Similarly digital forensic accounting play an important part in fraud examination as it helps in the preservation of evidence and enhance the trustworthiness of cyber-crime related investigation (Chalu, 2022). It is essential for the commercial banking sector since frauds such as online transfer, system breach, fraudulent transfer etc have occurred and are still occurring.

Another domain is concerned with the literature on fraud analytics, considered as a predictive and preventative tool of forensic accounting. Through the data driven method of analytics-including methods of identifying anomalous behaviour, of constructing behavioural models, of employing ratio analyses, time trends, and predictive risk models- fraud analytics focuses on predicting frauds to prevent them before significant losses occurs (Bhasin,

2022; Kassem and Higson, 2021; Vona, 2020). According to Bhasin (2022), fraud analytics enables banks to move away from their current trend of reactive fraud investigation to a system based on active prevention of fraud. Similarly, Kassem and Higson (2021) recognize that analytical predictive tools improve the detection of transactional anomalies, hidden behaviour anomalies and financial outliers. However, researchers emphasize its limit as well. Some of them argue fraud analytics may yield false positive results; it is said to be unable to operate without proper data quality, a proper digital infrastructure and the appropriate technical know-how (PwC, 2022; FATF, 2023). Nevertheless, its predictive feature for banking institutions is substantial.

The examination of financial statements has also been shown to have a remarkable degree of importance in forensic accounting literature. This includes searching for irregularities in the way accounting entries are recorded, liabilities are hidden, the assets are over-stated, revenues appear unusual, income is over-stated and fraud in financial statements (Rezaee and Wang, 2019; Vona, 2020; Crumbley et al., 2017). According to Rezaee and Wang (2019), fraud in financial statements is more often accomplished through trickery and skilful manipulation of accounting practices rather than actual theft. Vona (2020) suggests that forensic financial statement analysis will also distinguish between genuine accounting mistakes and outright fraud, this procedure is useful when looking at bank financial statements as the reliability of the banks statements affects trust for regulators and investors.

Other than financial statement analysis, forensic interviewing has been identified as an important investigative tool within forensic financial accounting. The approach in the practice of forensic interviewing requires the collection of data using methods of behavioural analysis and questioning (Van Graan et al., 2024; Murphy and Free, 2021). Murphy and Free (2021) suggests that the analysis of suspect behaviours and personal characteristics are important in the pursuit of financial fraud as the accused often tries to conceal their crimes by making excuses and employing interpersonal deception. The methodology in the practice of forensic interviewing will lead to increased reliability in the collected evidence and also make the evidence stronger for a defense in court (Van Graan et al., 2024). In the field of banking fraud, this procedure will be helpful because often there is insider colluding in a banking fraud investigation.

An important ongoing discussion in the forensic accounting literature is whether this practice should be treated mainly as a reactive mechanism post fraud or as a comprehensive governance approach. Initially in the literature, forensic accounting practice was discussed as mainly reactive in nature and dealing mostly with litigations and investigation after losses have occurred (Hopwood et al., 2012; Bologna and Lindquist, 1995). Modern scholars however are proposing that forensic accounting practice should be treated as a governance approach within fraud prevention mechanisms. Kassem and Higson (2021) argued that the forensic accounting practice enhances the governance function through increasing transparency and efficiency of the monitoring mechanisms and minimizing risks faced by institutions from fraud activities. Akinbowale et al. (2020) similarly showed that forensic accounting practice enhances institutional accountability and resistance. It means that modern approach recognizes the importance of strategic forensic accounting application in the context of banking governance.

Across Africa, implementation of forensic accounting is still a mixed bag of adoption despite increased fraud risk exposure. The ineffectiveness of its application continues to be hindered by lack of capacity, fragmented rules and regulation, digital infrastructure limitations, corrupt tendencies and less developed investigatory machinery (UNECA, 2020; FATF, 2023; World Bank, 2023). A study by Akinbowale et al. (2020) established that financial institutions in emerging African economies could be great beneficiaries with application of forensic accounting especially for preventing fraud and reinforcing resilience in corporate governance. Bhasin (2022) on his part suggests that African banking systems needed to embrace forensic accounting more because of the growing involvement of financial crime as a means to leverage loopholes in corporate governance structures.

Zimbabwe does, to some extent, mirror these institutional circumstances. The banking sector is undergoing and has recently experienced-an onslaught of digital transition; dependence on e-transactions; susceptibility to cyber fraud and failure of governance mechanisms in turbulent economic times (Reserve Bank of Zimbabwe, 2023; Mhlanga, 2024). Njanike and Mashayanye (2023) pointed out that poor internal controls; fractured governance mechanisms and institutional weaknesses lead to Zimbabwean banks being vulnerable to fraud. Notwithstanding this fact, there appears to be a lack of adequate literature on forensic accounting in Zimbabwean commercial

banking. Auditing, compliance and/or corporate governance-have been the focus of studies in this area, instead of application of integrated forensic accounting tools.

This body of literature therefore shows an obvious gap. Current research is largely fragmented as there are only specific studies focusing on transaction tracing, digital forensics, fraud analysis, governance or auditing. Few researches had combined these forensic accounting tools to an integrated forensic accounting system for detecting financial crime in Zimbabwean commercial banks. Therefore, this paper aims to eliminate this gap by integrating these forensic accounting methodologies into one investigative and governing system.

3. Theoretical Framework

The multifaceted nature of financial crime in commercial banks requires a substantial body of theory that explains motivation of fraud, the vulnerability of the institution, the failure of governance, behavioural malpractice, and financial manipulation opportunity. Forensic accounting is multidisciplinary as the identification and investigation of fraud typically involves; financial analysis, behavioural interpretations, accountability of institutions, legal evidence and risk management techniques. The present study thus draws on five interlinking theories; namely the Fraud Diamond Theory, Agency Theory, Routine Activity Theory, Behavioural Ethics Theory and Governance Theory, to strengthen the analytic basis of the study of how forensic accounting tools improve the detection of financial crime in Zimbabwean commercial banks.

The most pertinent theory in terms of explaining complex financial crimes is the Fraud Diamond Theory. Introduced by Wolfe and Hermanson (2004), it builds on the traditional Fraud Triangle, by considering capability an additional component that is necessary for fraud, along with pressure, opportunity, and rationalization. The theory posites that fraud can only occur if an individual has the right circumstances (incentives, opportunity), as well as capability to execute, in the form of technical competence, authority, ability, intelligence and confidence that enables them to capitalize on institutional weakness. In a commercial banking context, it is typically highly knowledgeable insiders, with the technical expertise to manipulate systems, issue fraudulent approvals, cover up evidence or to collude to commit fraud, who are the key players. Rezaee and Riley (2019) have said that financial fraud in regulated entities usually requires both opportunity and technical capability, in the presence of potential for leveraging digital systems to manipulate processes and data. Kassem and Higson (2021) adds that Forensic accounting must be used because the fraud tends to be a behavioural sophistication hidden within processes and transactions, rather than an obvious accounting anomaly. Fraud Diamond Theory therefore underlies the importance of forensic accounting methods that would trace the transactions, such as the use of digital forensic accounting and financial reconstruction.

Despite the prevalent use of Fraud Diamond theory, its potential limitations have led to some academic debates. Certain scholars consider the theory to focus on individual motivation drivers while overlooking institutional failure, governance and the overall structural vulnerability (Murphy and Free, 2021; Bhasin, 2022). Nevertheless, its contribution on capability still holds some relevance on the banking industry, in which fraudulent incidents often occur through insider exploitation, thus with necessary access rights and banking authorities.

Agency Theory has equally a great explanatory power of financial crime in commercial banking. The Agency Theory originally developed by Jensen and Meckling (1976) explains conflicts between a principal and agent when, as a result of asymmetry of information, self-interest, and poor monitoring, the agent will benefit individually at the expense of the institution. Managers, accountants, inside officers and controllers within a banking institution might know more about the operations than shareholders, boards, and depositors, hence opportunity for perpetration of fraud, off-book transactions, manipulation of account records, and insider dealing and arbitrary action. As Eisenhardt (1989) states agency conflict is greatest where monitoring is poor and incentives do not force the agent to act at the best interest of the principal, recent research by Njanike and Mashayanye (2023) revealed that weak governance and poor internal controls have led to an increase in vulnerability to fraud in the Zimbabwean financial institutions. From a forensic accounting viewpoint, Agency Theory may increase our understanding of the reason for transaction tracing, forensic audits, verification of evidences, and investigation on account of internal inquiry needed.

The principal criticism of Agency theory is that it is grounded on assumption of rational self-interest and may ignore the fact that ethical behaviour, cultural influence or institutional norms determine the way financial decisions is taken (Donaldson and Davis, 1991; Murphy and Free, 2021). In the internal hierarchy of banking organizations, information asymmetry, delegation and division of authority, this theory stands as a highly important theory in examining fraud risk.

Routine Activity Theory lends additional support to this research. In effect, institutional systems create opportunities for fraud, and according to Cohen and Felson (1979) crime is committed when a suitable target, motivated offender and lack of a capable guardianship are in convergence. Motivated offenders in financial systems might be insular employees, foreign cyber criminals, or insider/outsider collaborations. Suitable targets include the digitally conducted transactions, institutional capital, and customer deposits. Lack of capable guardianship includes inadequate internal controls, weak data security systems, and poor internal governance. Levi and Reuter (2006) state that financial crime has a tendency to thrive in areas with opportunity structures that can be exploited within a system. Similarly, Broadhurst et al. (2020) states that increased internet usage has expanded the cyber-opportunity exposure in digital banking. As such, forensic accounting procedures such as data analytics, transaction monitoring, digital forensics and evidence-based risk analysis are well supported because they act as additional capable guardians and consequently diminish opportunities for crime.

Although this theory offers clear explanation, Routine Activity theory was criticized due to emphasis on the situational opportunities and lack of behavioural ethics and institutional power (Yar, 2005; Murphy and Free, 2021). However, in banking institutions where fraud occurs in accordance to the opportunities that arise and lack of control systems, this theory is highly applicable.

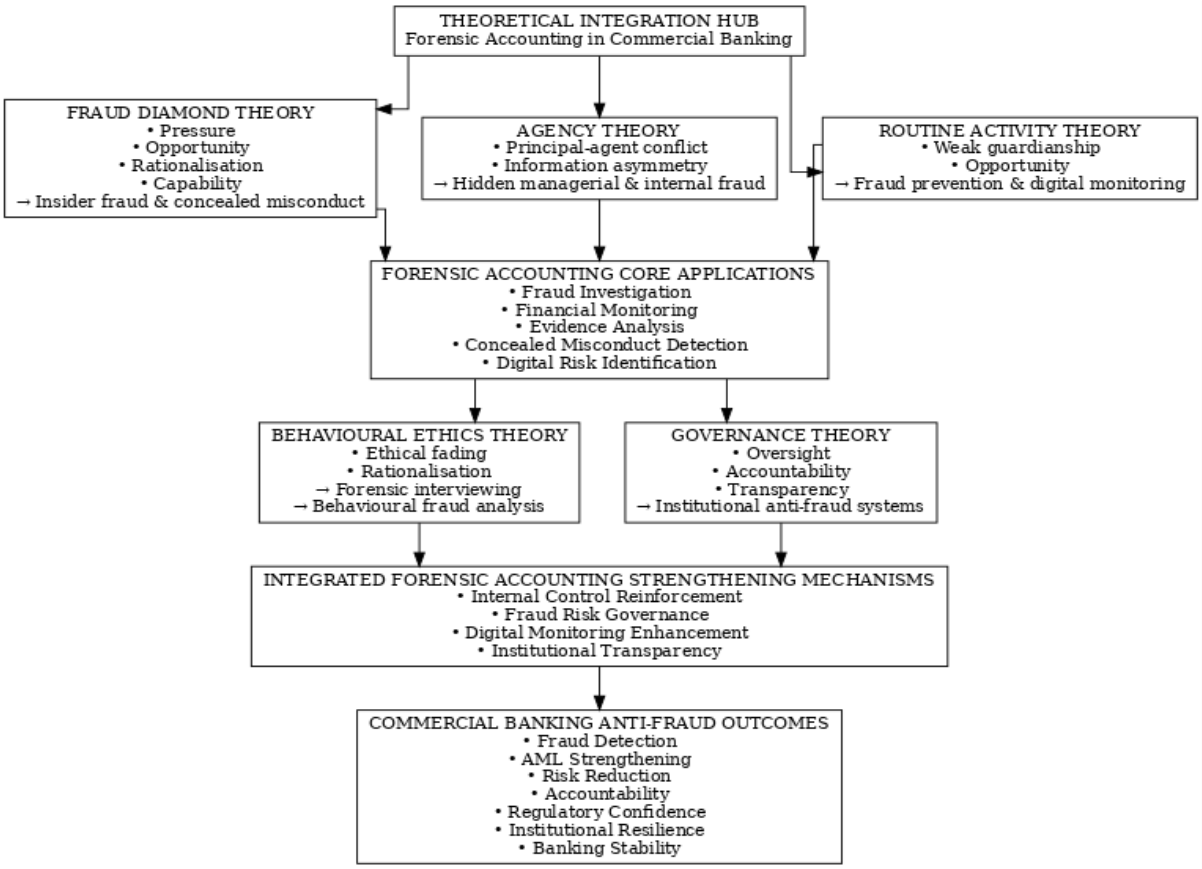
The concept of Behavioural Ethics Theory offers a key perspective on the ethical and psychological elements of wrongdoing. Financial crime is not simply the product of incentives and opportunity; but is often accompanied by phenomena such as moral disengagement, ethical fading, rationalisation and organisational normalisation of wrongful actions. According to Trevio et al. (2006), ethical behaviour is affected by both the individuals concerned and the environment they work within. Murphy and Free (2021), noted that unethical behaviour and subsequent financial misconduct arises when certain actions or conduct becomes normalised within an industry or organization; such as, where the practice of financial fraud can become so ingrained in a bank, employees rationalize the practice of manipulation, or cover-up errors, and justify unauthorised transactions as appropriate due to pressures to produce profit regardless of the costs to other stakeholders. In this situation, forensic accounting enhances an investigation by incorporating the study of behaviour, using forensic interviews and the critical analysis of evidence, together with an ethical analysis of the situation. Van Graan et al. (2024), noted that detection rates improve considerably when there is a structured format to the interviewing of potential suspects to ensure all their responses and behaviour patterns can be checked for consistency.

The limitation of Behavioural Ethics Theory is that ethics could differ within institutional cultures and, thus may not be consistent or easy to measure (Trevio et al., 2006; Murphy and Free, 2021). However, the theory is still valid as a considerable amount of banking fraud has been initiated by intentional rationalization and hidden misconduct.

Governance Theory is the last, and overarching theoretical approach. Governance Theory places high importance on: responsibility, vigilance, openness, the strength of internal control mechanisms, safeguarding stakeholders and institutional trusteeship (Tricker, 2015; Solomon, 2021). For the banking system, the internal governance mechanisms of the institution will impact on; internal fraud prevention, the monitoring mechanisms in place, the existence of segregation of duties, the robustness of compliance and the strength of accountability measures. The existence of poor governance enhances chances of fraud; concealed transactions and weak institutional oversight. According to Solomon (2021), governance is at the root of the vast majority of large financial scandals. This was also echoed by Akinbowale et al. (2020) who found that forensic accounting can enhance institutional governance resilience, and this can be attributed to reliable evidence and accountability mechanisms. Considering the weaknesses in governance and weak institutional oversight in commercial banks in Zimbabwe, governance theory heavily supports the incorporation of forensic accounting into the institution.

The way in which the above theories contribute to an overall understanding of forensic accounting relevance need to be articulated together in order to draw the theoretical perspective of these theories on banking fraud. Figure 1, outlined below summarizes the theories under this study.

Figure 1: Theoretical Integration and Relevance to Forensic Accounting in Commercial Banking



Source: Synthesised from Wolfe and Hermanson (2004), Jensen and Meckling (1976), Cohen and Felson (1979), Murphy and Free (2021), and Solomon (2021).

From the theoretical combination (Figure 1), it is evident that, financial crime occurrence in the commercial banking sector cannot be explained by a single theory. There can be an instance of the occurrence of fraud through capability, opportunity, ethical failure, agency conflict or poor governance. Hence, forensic accounting approaches to the identification of such crimes are, or should be multidisciplinary and combine all the applicable techniques.

To summarize the applicability of the theories, when seen together, these theories adequately explain the application of forensic accounting in enhancing the detection of financial crime in commercial banks of Zimbabwe. Frauds are detected through the technical capacity and hidden misconduct of agents using Fraud Diamond Theory, through hidden conflicts and information asymmetry between parties using agency theory, through weak or available opportunity using routine activity theory, and through a failure to uphold ethical standards using behavioural ethics theory, while the presence of robust governance ensures adequate accountability and control using governance theory. Their convergence explains why there is need for the comprehensive forensic accounting investigation framework.

4. Methodology

This research employed a conceptual and evidence-based review method to critically analyse the extent to which forensic accounting techniques enhance detection of financial crimes in commercial banks of Zimbabwe. A conceptual review method was employed as the research seeks to bring together theory, practice and institutions rather than collecting new primary data. The area of banking crime detection involves an interplay of accounting,

fraud governance, criminology, auditing, digital forensics, law and institutions. Thus, an evidence-based structured review helped to consolidate fragmented research findings into an analytical investigative framework for commercial banking contexts (Snyder, 2019; Booth et al., 2021; Saunders et al., 2019).

Conceptual reviews are increasingly favoured in accounting, governance and financial crime studies as they promote thorough conceptual integration and critical interpretation of fragmented literature. Snyder (2019) regards evidence-based literature reviews as useful in developing a conceptual clarity, identify knowledge gaps, and synthesize fractured knowledge in multidimensional research areas. Torraco (2016) asserts that an integrative conceptual review leads to enhanced theory construction by connecting existing empirical knowledge to unresolved practical and academic questions. This research found a conceptual review particularly useful in bringing together separate aspects of financial crime detection such as fraud analytics, digital forensics, auditing, anti-money laundering systems and governance, to create one broad investigative framework since many existing studies treat each aspect in isolation.

The philosophical approach taken for this study was interpretivist and analytical. While interpretivism is often applied to qualitative research, it can also be applied to conceptual reviews where the intention is to identify meaning, relationship and contextual importance within the scholarly literature rather than statistically measuring variables (Creswell and Creswell, 2018; Bryman, 2021). The research thereby sought to understand the arguments for the application of forensic accounting methods, the theoretical underpinnings for the use of such techniques in financial crime detection in banks and the overall institutional resilience and accountability aspects of using forensic accounting.

In this study only secondary sources of data were utilized. The sources utilized included peer-reviewed journal articles, corporate reports by institutions dealing with anti-financial crime, forensic accounting studies, literature on banking governance, reports on anti-money laundering, reports on financial crimes. Quality and traceable sources from credible institutions and reputable journal such as *Journal of Financial Crime, Managerial Auditing Journal, Meditari Accountancy Research, Accounting, Organizations and Society, International Journal of Accounting & Information Management, the Association of Certified Fraud Examiners, Financial Action Task Force, World Bank and Reserve Bank of Zimbabwe* were given priority. It has been said that careful selection of the sources to draw data from can lend weight to the study (Saunders et al., 2019), and filtering quality can increase the reliability of the conceptual synthesis (Snyder, 2019).

To gather evidence in a systematic manner a literature search strategy was implemented. The search strategy consisted of search for studies on forensic accounting, financial crime detection, banking fraud, digital forensic accounting, anti-money laundering investigation, fraud analytics, governance failure and commercial banking fraud. Search terms utilized included forensic accounting techniques, banking fraud detection, digital forensic accounting, anti-money laundering investigation, financial crime in banks, Zimbabwe banking governance. This strengthened relevance and thematic unity of the literature sourced. A structured literature search helps in providing transparency in research and avoiding arbitrary selection of literature (Booth et al., 2021).

To bring scientific vigor to the analysis, criteria for inclusion were used. First the studies needed to be relevant in direct terms to the concepts of forensic accounting, fraud detection, financial crime investigation, anti-money laundering system, accountability and banking fraud. Second, the criteria were centred on modern literature since there has been a rapid increase in digital financial crime globally, and where there are no contemporary sources covering a particular aspect, the seminal studies are included if they are of relevance to the theory. Third, studies from global, African and Zimbabwean environment were taken into consideration, to accommodate the funnel approach in the analysis. Fourth, sources needed to be of credible institutions and peer-reviewed so as to be traceable (Saunders et al., 2019; Booth et al., 2021).

Simultaneously, exclusion criteria had to be set to avoid overwhelming the analysis. Studies which do not pertain to financial institutions, general discussions of corporate governance without relation to fraud, sources which are not of high quality and therefore not traceable, and generally literature on criminal justice or general cybercrime

without relation to accounting, fraud investigation and banking were eliminated. This also ensures that the analysis remains theme oriented.

Thematic analytical synthesis was used as the analysis strategy in this study. Thematic synthesis is especially appropriate in a conceptual study because it allows repeated concepts, relationships and theoretical elements to be categorized and synthesized systematically (Thomas and Harden, 2008; Snyder, 2019). The researcher analysed the chosen articles and developed consistent themes relating to detecting financial crime and the importance of forensic accounting. The main themes were: Forensic accounting as a governance mechanism, Transaction tracing, Digital forensic accounting, Fraud analysis, financial statement analysis, Forensic interview, Anti-money laundering investigations, Asset tracing, behavioural vulnerability, governance failure, institutional resilience. Synthesising these recurrent themes, the researcher was able to create an Integrated Forensic Accounting Investigative Framework that is relevant to Zimbabwean commercial banks. To give an illustration of the thematic analytical direction that guided the review, it is important to give a summation of the major analytical themes from literature and their importance to the study. Major analytical themes are shown in Table 1.

Table 1: Major Analytical Themes Used in the Evidence-Based Review

		EVIDENCE-BASED REVIEW SYNTHESIS HUB Strategic Analytical Integration						
			↓	↓	↓			
TRANSACTION TRACING AML strengthening Concealed flow reconstruction			**DIGITAL FORENSIC ACCOUNTING** Cyber-financial crime detection Electronic trails			**FRAUD ANALYTICS** Predictive fraud identification Pattern modelling		
	↘			↓			↙	
		FORENSIC ANALYTICAL CORE Financial Statement Analysis Manipulation Detection Reporting Fraud Identification Behavioural & Evidential Interpretation						
				↓				
	FORENSIC INTERVIEWING Behavioural analysis Evidential reliability				**GOVERNANCE FAILURE** Weak controls Institutional vulnerability			
		↘		↓		↙		
		INSTITUTIONAL RESILIENCE Strategic anti-fraud capacity Governance strengthening Banking sustainability						
				↓				
	IMPROVED FRAUD GOVERNANCE OUTCOMES Fraud Detection AML Effectiveness Risk Reduction Institutional Accountability Strategic Resilience Regulatory Confidence Banking Stability							

Source: Developed from research synthesis based on reviewed literature.

The themes illustrated in Table 1 exhibit the multi-faceted approach used in financial crime investigations within banks. These themes further highlight how forensic accounting is moving beyond simply a focus on investigating fraud and encompassing areas such as governance, digital analysis, evidentiary value and organizational resilience.

Methodological trustworthiness was approached through conceptual alignment, transparency, source validation and thematic coherence of analysis, thereby increasing the robustness of the study. According to Lincoln & Guba (1985), credibility, dependability, confirmability and transferability are central aspects of qualitative research. Though this was not an empirical, field-based qualitative study, principles akin to those suggested by Lincoln and Guba (1985) underpinned the process of literature review and synthesis. Credibility was attained through a critical review of peer-reviewed academic journals and institutional sources. Dependability was ensured through clear criteria for literature selection and through the cohesive manner in which themes were integrated. Confirmability was assured through providing evidence to support the interpretations made, as opposed to abstract analysis. Transferability was achieved by encompassing international, African, and Zimbabwean banking perspectives to illustrate the applicability of the research findings.

A constraint inherent to the methodology of conceptual review is that primary empirical data from the banking environment are not produced as part of the research process. Research findings are based on the interpretation of secondary data, rather than direct interaction with institutions (Bryman, 2021; Creswell & Creswell, 2018). Strengths of this approach include theory-building, integration of various sources of knowledge and creation of an investigative model. The methodology of this study lent itself perfectly to the goal of critically investigating and then synthesising different techniques used in forensic accounting and of developing an integrated framework for forensic investigation.

5. Findings and Critical Discussion

It has emerged from the evidence-based review that forensic accounting techniques enhances detection of financial crimes, strengthens accountability, increases resilience and bolsters fraud investigations in commercial banks. However, the findings indicates that the effectiveness of forensic accounting rests on combinations of technological capability, governance strength, digital readiness, institutional commitment and integrated multidisciplinary investigative system. Financial crimes in commercial banks are becoming multidimensional-with behavioural manipulation, digital concealments, internal collusions, transaction complexities and institutional governance failures occurring. As such, single, anti-fraud systems might not be capable of deterring sophisticated financial crime.

The most important discovery of the research is that transaction tracing is one of the most significant forensic accounting techniques for the detection of financial crime in banking institutions. The evidence confirms consistently that money laundering, illicit transfers, related-party transactions that have been concealed and concealed movement of assets are structured in a fragmented manner with a view to concealing information regarding the owner and origin of the transaction (Manning, 2019; FATF, 2023; Levi and Reuter, 2006). In Zimbabwean commercial banks with proliferation of digital transactions, mobile money transfer and movement of money across various institutions, the transaction tracing technique may improve the reconstruction of suspected movements of funds and enhance anti-money laundering investigation. This is consistent with Fraud Diamond Theory and Agency Theory whereby the knowledgeable actor might use technological access and institutional opportunity to conceal transactions while hidden information asymmetry facilitated by Agency Theory, enables internal financial malfeasance (Wolfe and Hermanson, 2004; Jensen and Meckling, 1976). Therefore, transaction tracing technique may contribute in the prevention of concealments.

The study findings indicate that the practice of digital forensic accounting is central in modern banking fraud investigations. Growth of e-banking, internet based financial transactions, mobile payment systems and automatic money transfer have moved considerable business transactions to digital domain. While this has brought about operational efficiencies, it has consequently created vulnerabilities to cyber financial crime, phishers, ransomware

agents, fraudsters and manipulation through digital domain (Broadhurst et al., 2020; PwC, 2022; Mhlanga, 2024). Digital forensic accounting aids in improvement of fraud investigations due to analysis of metadata, electronic audit trail, logs of system access, date and time data, erased information, and altered system data (Albrechtsen, 2020; Chalu, 2022).The finding aligns closely with Routine Activity Theory on the fact that digital financial systems may be viewed as exploitable opportunity structure where weak guardianship increases the potentiality for fraud (Cohen and Felson, 1979). The rapid digital expansion in Zimbabwean commercial banks may heighten vulnerabilities in the absence of cyber-forensic readiness.

A further significant discovery is that fraud analytics enables the provision of predicted and proactive fraud detection. Traditionally, fraud management systems tend to identify the fraud loss after it has already occurred; hence, they are often reactive. However, fraud analytics allows for the detection of fraudulent activity through identification of anomalies, behavioural modelling, identification of transaction outliers, usage of prediction algorithms, and pattern identification (Vona, 2020; Kassem and Higson, 2021; Bhasin, 2022). The research revealed that it enables banks to effectively identify hidden irregularities, repetition of the fraud, and deviant financial transactions before the crime reaches maturity. In line with the Governance Theory, fraud analytics is a monitoring technique that enhances transparency and accountability of management in banks (Solomon, 2021); however, literature notes limitations in relation to lack of infrastructure, poor quality data and technical expertise as potentially impacting on the practice especially in emerging economies (PwC, 2022; FATF, 2023). This indicates that it requires the involvement of institutions to realize full benefit.

The study also established that financial statement analysis is vital in detecting hidden accounting manipulation and reporting fraud. Financial reports are central for banks for reporting, compliance, liquidity, operational transparency and investor assurance. Manipulation through financial reporting could manifest itself in hidden liabilities, understated or over stated assets, exaggerated profits or losses and distorted disclosures (Rezaee and Wang, 2019; Crumbley et al., 2017; Vona, 2020). Financial statement analysis enables the discrimination between accounting irregularities and intentional manipulation of financial statements. This finding corroborates Agency Theory wherein fraud may be committed where there are a conflict of interest and a lack of transparency among the internal parties (Jensen and Meckling, 1976; Eisenhardt, 1989). The analysis of financial statements plays a significant role particularly in the banks that face uncertainties and increased scrutiny under varying economic situations such as in Zimbabwe.

Another significant finding relates to forensic interviewing which is a behavioural and evidential technique. Fraud, cannot always be captured by quantitative financial figures as often relies on rationalization, deception, ethical fading and deliberate concealment of the fraud. The literature explains that well-structured forensic interviewing of suspects and other related parties enhances reliability of evidence, exposes inconsistencies in information and allows for behavioural interpretation during fraud investigation (Murphy and Free, 2021; Van Graan et al., 2024). This finding directly relates to Behavioural Ethics Theory whereby financial wrongdoing may transpire as a result of rationalization, moral decay and institutional condoning of ethical compromise (Trevio et al., 2006; Murphy and Free, 2021). In banking institutions, internal collusion might arise making forensic interviewing crucial in corroborating evidence and understanding behavioural risk indicators.

To further consolidate the major forensic accounting techniques identified and their role in financial crimes investigation in banking institutions, the analytical findings have been summarized below. Table 2 outlines the main forensic accounting techniques and institutional implications to financial crime detection.

Table 2: Major Forensic Accounting Techniques and Their Role in Banking Fraud Detection

	BANKING FRAUD DETECTION SYSTEM (Core Investigative Governance Hub)			
	↓	↓	↓	

TRANSACTION TRACING Suspicious fund flows Hidden transfers AML detection	DIGITAL FORENSIC ACCOUNTING Electronic evidence Cyber-fraud reviews Unauthorized transfers	FRAUD ANALYTICS Predictive detection Early alerts Pattern analysis	FINANCIAL STATEMENT ANALYSIS Manipulation Reporting fraud Accountability	DOCUMENT EXAMINATION Authenticity Audit trail Record integrity
↓	↓	↓ RELATIONSHIP FLOW ↓	↓	↓
FORENSIC INTERVIEWING Behavioural evidence Insider fraud Test reliability	EVIDENCE PRESERVATION Legal defensibility Litigation support Chain of custody	ASSET TRACING Concealed assets Recovery Accountability	DATA MINING Hidden patterns Large data review Risk signals	BENFORD'S LAW ANALYSIS Anomaly spotting Numerical fraud Validation
↘	↘	↓	↙	↙
GOVERNANCE & BANKING OUTCOMES Transparency Compliance AML Strengthening Fraud Recovery Institutional Accountability Risk Reduction Banking Stability Resilience				

Source: Research synthesis based on reviewed literature.

The findings in Table 2 support the fact that forensic accounting is multifaceted rather than just a daily examination of fraud. It includes elements of digital forensics, behavioural analysis, corporate accountability, management of legal evidence and financial tracing, confirming that effective banking fraud identification systems are holistic and cross-functional.

Another significant finding of this research is that weak governance is arguably the most potent barrier to the effective implementation of forensic accounting. Existing literature is replete with research linking increased fraud exposure with weak internal controls, lack of segregation of duties, lack of coherent supervision, lack of accountability, and lack of effective implementation of corporate mechanisms (Akinbowale et al., 2020; Solomon, 2021; Njanike and Mashayanye, 2023). The theory of Governance directly explains the relation; weak governance leads to decrease in guardianship and increase in opportunities to perpetrate fraud. In the context of Zimbabwean commercial banks, weak governance can undermine effectiveness of forensic accounting despite the availability of relevant technological tools.

The study found that, forensic accounting can best be understood as a strategic mechanism for corporate governance instead of a limited technique for detecting financial fraud post-facto. Early researchers considered forensic accounting primarily as a reactive element primarily used to support litigation, and to measure the extent of fraud and loss incurred (Hopwood et al., 2012; Bologna and Lindquist, 1995). However, recent researchers have posited the importance of the preventive and governance-driven aspect of forensic accounting. According to Kassem and Higson (2021), forensic accounting has the capacity of increasing institutional transparency, resilience against fraud and an effective tool of supervision. Akinbowale et al. (2020) on the other hand found that forensic accounting can boost the level of accountability and effectiveness of anti-fraud mechanisms. This transformation is critical considering that strong governance mechanisms are imperative for sustainable resilience of the banking sector in Zimbabwe.

6. Integrated Forensic Accounting Investigative Framework

The study results reveal that partial anti-fraud mechanisms cannot combat the detection of financial crime within commercial banking institutions. Banking financial crime is growing, with increasing sophistication to digitally conceal financial crimes, influence behaviour, connive, create complexity of transactions, breakdown in governance and information asymmetry. Consequently, the study recommends an Integrated Forensic Accounting Investigative Framework (IFAIF) that seeks to bolster financial crime detection in Zimbabwean commercial banks. The IFAIF emanates from the synthesis of study findings, forensic accounting literature and the five underlying theories namely: Fraud Diamond Theory, Agency Theory, Routine Activity Theory, Behavioural Ethics Theory and Governance Theory.

The proposed framework conceptualizes financial crime detection as an integral and interdependent process as opposed to a discrete investigative intervention. Earlier research on forensic accounting posited forensic accounting as essentially a post-fraud activity connected to the Litigation Support role, Evidence Collection and the Determination of financial losses (Hopwood et al., 2012; Bologna and Lindquist, 1995). Current research indicates that the role of forensic accounting must now be part of the organizational control structure (internal control, fraud prevention and governance) and also strategic monitoring function (Kassem and Higson, 2021; Akinbowale et al., 2020; Bhasin, 2022). This research agrees on the above and therefore presents the view that forensic accounting is both investigative and governance discipline.

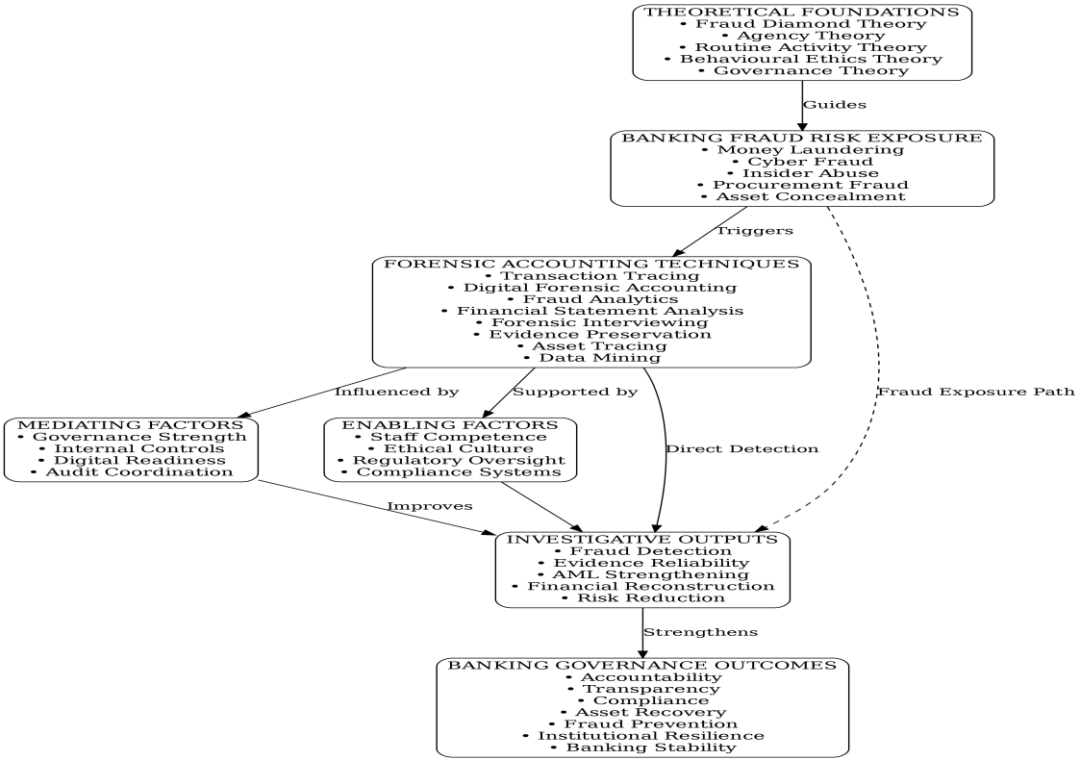
The IFAIF commences with the concept of financial crime risk exposure; this is considered to be the primary fraud environment confronting commercial banks. Major financial crime risk categories are identified as money laundering, cyber-financial crime, insider abuse, procurement fraud, unauthorized electronic transfers, asset concealment, related-party manipulation and financial statement fraud, which tend to emerge under weak governance, digital vulnerabilities, information asymmetry, behavioral failure, and internal collusion (Levi and Reuter, 2006; FATF, 2023; Njanike and Mashayanye, 2023). Fraud Diamond Theory explains the manifestation of these fraud risks using concepts of opportunity, rationalization, pressure, and capability; whereas Agency Theory can explain how the risk becomes more intensified by the existence of hidden information asymmetry (Wolfe and Hermanson, 2004; Jensen and Meckling, 1976).

The second phase of the framework deals with the application of forensic accounting investigative mechanisms; these may be defined as the operational and evidentiary response to the observed financial crime risks. Transaction tracing, digital forensic accounting, fraud analytics, forensic accounting analysis of financial statements, forensic interviewing, evidence preservation, financial reconstruction and asset tracing are identified as some of the key forensic accounting tools in banking investigations (Manning, 2019; Vona, 2020; Kassem and Higson, 2021). These tools have been identified to improve the visibility of financial fraud, enhance the quality of evidence and increase the institutional ability to reconstruct concealment activities (Cohen and Felson, 1979).

The third part deals with the incorporation of governance and internal control system, which will serve as supplements to forensic accounting tools and techniques for the fight against fraud. The research suggests that although forensic accounting is important, forensic accounting investigations should be backed by effective internal governance mechanism. Segregation of duties, interaction of internal audit, reporting of unusual transactions and digital surveillance system and legal/ institutional liability within a governance structure would enhance efficacy (Solomon, 2021; Akinbowale et al., 2020; Njanike and Mashayanye, 2023). However, lack of good governance structure will limit the relevance of forensic accounting investigative tools, resulting in poor monitoring and lack of teamwork in the investigative process (Governance Theory).

The fourth phase is related to the investigation and legal outcomes of financial crime detection; this is the ultimate objective of integrating forensic accounting in institutional governance, thereby achieving a greater level of financial fraud detection, stronger and reliable evidence, more effective anti-money laundering controls, asset recovery, as well as enhanced support for litigation and legal processes and ultimately, greater institutional transparency and resilience to financial fraud (Rezaee and Riley, 2019; FATF, 2023). To illustrate these inter-connected phases, the proposed framework is summarized below.

Figure 2: Integrated Forensic Accounting Investigative Framework (IFAIF)



Source: Developed by the researcher from empirical synthesis and theoretical integration.

In essence, as illustrated in Figure 2, financial crime detection is a staged and interconnected process. Financial crime risk exposure leads to institutional exposure; investigative response from the use of forensic accounting processes enhances investigation; institutional control from governance alignment strengthens institution and response; and accountability and enforcement from investigation enhance prosecution and banking soundness.

One significant benefit that this framework offers is that it presents the adoption of forensic accounting from the fraud-investigative perspective to a proactive governance-based model. Given the pervasive increase in fraud risks within Zimbabwean commercial banks, as a result of the volatile macro-economic conditions, fragmented governance, digital transformation and weakness in institutional controls (World Bank, 2023; Mhlanga, 2024; Njanike and Mashayanye, 2023), the IFAIF thus offers a model specific to the environment.

Furthermore, this framework attempts to address the gap in forensic accounting literature. Several pieces of literature analyze fraud analytics, digital forensic accounting, evidence trail and transaction tracing or governance separately (Bhasin, 2022; Chalu, 2022; Kassem and Higson, 2021). Very few studies attempted to merge these disciplines into one single forensic accounting framework for the purposes of detection of fraud in the banks, specifically in emerging countries. This work contributes conceptually by addressing that gap.

The Practical implication of the IFAIF is vast; Zimbabwean commercial banks could utilize this framework in enhancing the anti-money laundering investigation process, digital fraud detection, preservation of evidence, regulatory compliance and strategic fraud governance. Furthermore, regulators, like the RBZ, as well as anti-money laundering agencies could adopt this model to better oversee the sector.

The Integrated Forensic Accounting Investigative Framework provides an integrated and multidimensional model for reinforcing the investigation of financial crimes within Zimbabwean commercial banks, and lends weight to the idea of integrating forensic accounting as a tool of strategic governance.

7. Practical Implications

The findings of this study have significant practical implications for commercial banks, regulators, forensic investigators, auditors, anti-money laundering organizations and policymakers in Zimbabwe. This study argues that forensic accounting cannot only be a mere technical tool for investigative purposes but can also serve as strategic tool that enhance the identification of fraud, the governance accountabilities, the financial strength of an institution, and transparency. Due to increasingly sophisticated nature of fraud in banking institutions, greater integration of forensic accounting in both governance and operative systems becomes vital.

One of the major implications for Zimbabwean commercial banks is to move beyond the current conventional audit system and institutionalize dedicated forensic accounting functions within their structures. Even though internal audit is significant in checking the compliance aspect and evaluating controls, conventional auditing does not provide the depth in detecting hidden fraud, manipulation in data, related-party transactions, and laundering complex operations (Rezaee and Riley, 2019; Vona, 2020; Kassem and Higson, 2021). Forensic accounting functions in the forms of dedicated departments/units would enhance systematic fraud investigations, the handling of evidence, digital review, and asset recovery. This would not only promote investigative specialization but also responsiveness to fraud.

Another key implication is for the commercial banks to beef up transaction tracing mechanism and anti-money laundering investigations. Financial crimes are often characterized by indirect money movements, layering operations, hidden relationships among stakeholders, and fragmentation of financial streams which may bypass normal surveillance systems (Manning, 2019; FATF, 2023; Levi and Reuter, 2006). Hence, it is essential that transaction tracing becomes an integral part of reconstructing suspicious transactions to uncover the relationship among them. Given the rise in digital transactions and mobile money services in Zimbabwe, a reinforced tracing system would enhance money laundering detection as well as the visibility of fraud.

An important implication relates to the readiness of the commercial banks on digital forensic accounting. The facts presented have shown beyond doubt that banking fraud is now moving into the electronic sphere in the form of electronic funds transfers fraud, cyber financial crime, phishers, ransomware attacks and digitally altered records (identity). Commercial banks need to develop digital forensic capacities. These could be in terms of electronic evidence preservation, real-time logging and monitoring, meta-data and access trail data analysis, cyber fraud reconstruction. In the absence of readiness on this side, the significant volume of banking fraud may go undetected by contemporary conventional audit/investigation methods.

A further implication is to integrate fraud analytics into a pre-emptive fraud governance system. Fraud analytics plays an essential role in pre-emptive detection of fraud, since the systems are designed to spot out anomalies, monitor the conduct of parties in an operation, detect unusual transactions and predict the likelihood of certain fraud occurrences based on statistical models (Bhasin, 2022; Kassem and Higson, 2021; Vona, 2020). Instead of just detecting fraud after financial losses have already been incurred, commercial banks ought to institutionalize pre-emptive fraud analytics to provide early warning signals. This is particularly applicable in Zimbabwe as it faces its own economic turmoil and increasing use of digital systems by consumers of financial services, thereby posing a heightened risk of fraud.

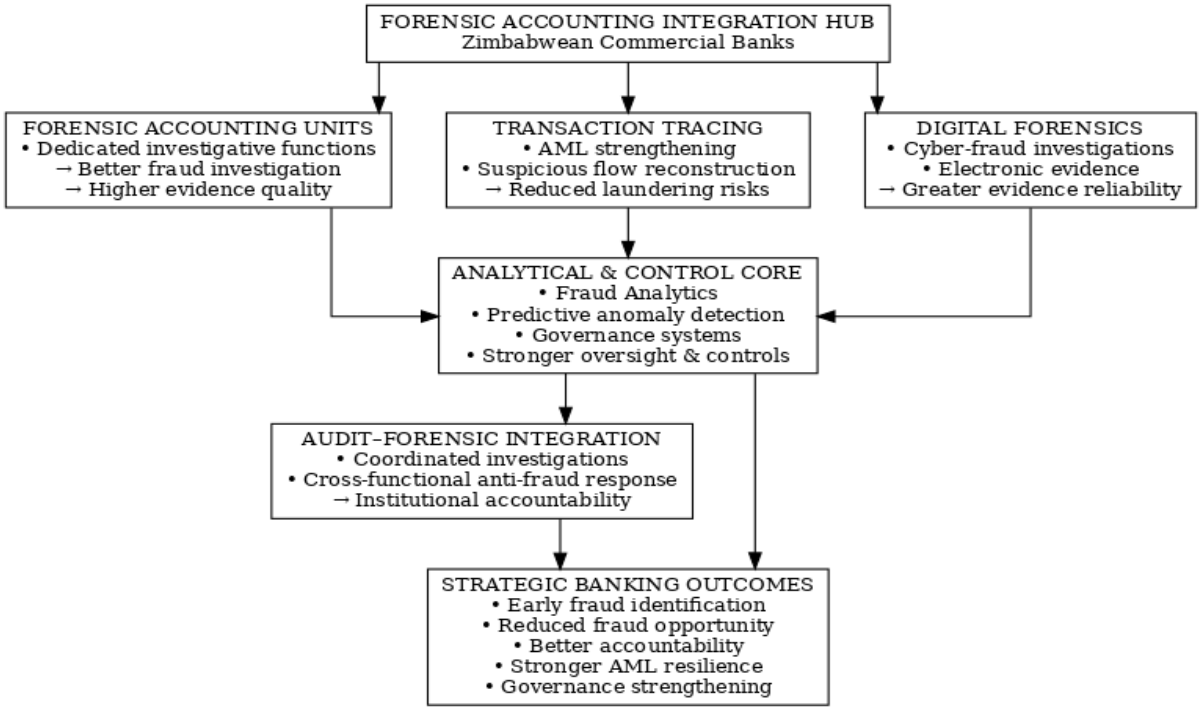
The integrity of governance is also a major institutional implication. The presence of weakly laid internal controls, lack of coordination in overseeing the entire system of fraud, the disregard of appropriate separation of duty, and low accountability would continue to undermine forensic accounting regardless of its availability and potential for use in controlling fraud (Akinbowale et al., 2020; Solomon, 2021; Njanike and Mashayanye, 2023). Therefore, commercial banks should focus on enhancing governance mechanisms for forensic accounting, that includes strengthened internal controls, proper fraud investigation channels, Board-level support, better coordination among audit functions and forensic accountants, compliance measures and accountability mechanisms.

Forensic investigators and auditors are not left out either in the implications derived from this research. Internal auditors, external auditors and forensic investigators must foster integrated anti-fraud systems since although conventional auditing functions can detect an anomaly, forensic accounting goes a step further by focusing on

evidence-based investigations (Messier et al., 2017; Rezaee and Wang, 2019; Vona, 2020). The collaboration between audit processes and forensic accounting units will ensure better fraud verification, enhanced integrity of evidence and legal defensibility of any investigation.

To provide a clear synthesis of the practical implications of the study at an institutional level, a summary is presented on Figure 3.

Figure 3: Practical Implications of Forensic Accounting Integration in Zimbabwean Commercial Banks



Source: Developed by the researcher from findings synthesis.

The deductions from Figure 3 enhance the claim that forensic accounting supports technical investigation of fraud, as well as banking governance in general. These types of mechanisms can influence both institutional soundness and susceptibility to fraud. The deductions from Figure 3 also have important lessons for the Reserve Bank of Zimbabwe. Regulators of banks must promote stricter forensic accounting practices, digital fraud preparedness and the mechanisms of investigating the fraud. These measures of regulatory framework could be influential in enhancing institutional resilience to fraud through greater anti-money laundering review, evidential retention mechanism, fraud reporting mechanism and coordinated forensic audits (Reserve Bank of Zimbabwe, 2023; FATF, 2023; World Bank, 2023). A sweeping change in the banking governance across the industry would be useful in improving institutional comparability.

From a national level perspective, lessons can be derived for institutions of higher learning and accounting professional bodies to upgrade their standards for forensic accounting training. As the system of banking and financial transaction mechanism evolves toward digital and online system in Zimbabwe, competent personnel with multi-disciplinary investigative tools such as fraud analytics, digital forensics, financial re-construction, behavioural investigation, and evidential assessment (Akinbowale et al., 2020; Bhasin, 2022; Chalu, 2022) are needed. Forensic accounting training of professionals would enable institutions to become long-term fraud ready.

8. Conclusion

This study has critically explored how forensic accounting techniques enhances the detection of financial crimes in Zimbabwean commercial banks. Financial crime continues to represent one of the most resilient threats to institutional legitimacy, banking stability, governance quality and financial resilience. Modern fraud trends are

often motivated by technology transformation, internal collusion, hiding of transactions, weak governance and macroeconomic uncertainty hence demanding greater investigative and governance-based responses than merely conventional financial controls.

This study concludes that forensic accounting has emerged as an investigative and governance discipline. Transaction tracing, digital forensic accounting, fraud analytics, financial statement analysis, forensic interviewing, preservation of evidence, asset tracing and financial reconstruction significantly improve fraud detection, anti-money laundering investigations, integrity of evidence, asset recovery and institutional accountability (Manning, 2019; Rezaee and Wang, 2019; Kassem and Higson, 2021). All these tools contribute in building a stronger framework for both preventive and investigative fraud governance.

Furthermore, the study established that good governance is the ultimate underpinning in making forensic accounting effective. Poor controls, weak supervision, disintegrated accountabilities and poor digital readiness of commercial banks may undermine the anti-fraud effectiveneness of forensic accounting, even where available (Akinbowale et al., 2020; Solomon, 2021; Njanike and Mashayanye, 2023). Forensic accounting has therefore to be intrinsically intertwined in good institutional governance structures.

A key contribution of this study is the establishment of the Integrated Forensic Accounting Investigative Framework (IFAIF) that interlinks financial crime risk exposure, the use of forensic accounting tools, the integration into governance and the investigative outcome. This framework will build understanding of forensic accounting as a strategic institution defense tool instead of a mere response to a post fraud issue.

In the Zimbabwean context, commercial banks will need increased institutionalization of forensic accounting, enhance digital forensic readiness, improve governance practices, build strong fraud analytics capacity, and enhance integration into the anti-money laundering regime. This can only be realised if all stakeholders including regulators, auditors, accounting bodies and educational institutions play their role.

References

1. ACFE (2022), *Occupational Fraud 2022: A Report to the Nations*, Association of Certified Fraud Examiners, Austin, TX. Available at: https://www.acfe.com/report-to-the-nations/2022/ (Accessed 15 May 2026).
2. Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020), "An innovative approach in combating economic crime using forensic accounting techniques", *Journal of Financial Crime*, Vol. 27 No. 4, pp. 1253–1271. https://doi.org/10.1108/JFC-04-2020-0053
3. Albrechtsen, E. (2020), "Digital forensics and cybercrime investigation in financial systems", *Computers & Security*, Vol. 92, 101760. https://doi.org/10.1016/j.cose.2020.101760
4. Arner, D.W., Barberis, J. and Buckley, R.P. (2020), "FinTech and the future of finance", *Journal of Banking Regulation*, Vol. 21 No. 1, pp. 1–13. https://doi.org/10.1057/s41261-019-00103-1
5. Bhasin, M.L. (2022), "Forensic accounting and fraud detection: Empirical evidence in financial institutions", *Managerial Auditing Journal*, Vol. 37 No. 5, pp. 610–628. https://doi.org/10.1108/MAJ-11-2021-3362
6. Bologna, G.J. and Lindquist, R.J. (1995), *Fraud Auditing and Forensic Accounting: New Tools and Techniques*, Wiley, New York.
7. Booth, A., Sutton, A. and Papaioannou, D. (2021), *Systematic Approaches to a Successful Literature Review*, 3rd ed., Sage, London.
8. Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2020), "Organizations and cybercrime: An analysis of financial system vulnerabilities", *International Journal of Cyber Criminology*, Vol. 14 No. 1, pp. 1–21. https://doi.org/10.5281/zenodo.3760116
9. Bryman, A. (2021), *Social Research Methods*, 6th ed., Oxford University Press, Oxford.
10. Chalu, H. (2022), "Digital forensic accounting and cyber fraud prevention in financial institutions", *International Journal of Accounting & Information Management*, Vol. 30 No. 3, pp. 345–362. https://doi.org/10.1108/IJAIM-07-2021-0154

11. Cohen, L.E. and Felson, M. (1979), "Social change and crime rate trends: A routine activity approach", *American Sociological Review*, Vol. 44 No. 4, pp. 588–608. https://doi.org/10.2307/2094589
12. Creswell, J.W. and Creswell, J.D. (2018), *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, 5th ed., Sage, Thousand Oaks.
13. Crumbley, D.L., Heitger, L.E. and Smith, G.S. (2017), *Forensic and Investigative Accounting*, 8th ed., CCH, Chicago.
14. Donaldson, L. and Davis, J.H. (1991), "Stewardship theory or agency theory: CEO governance and shareholder returns", *Australian Journal of Management*, Vol. 16 No. 1, pp. 49–64. https://doi.org/10.1177/031289629101600103
15. Eisenhardt, K.M. (1989), "Agency theory: An assessment and review", *Academy of Management Review*, Vol. 14 No. 1, pp. 57–74. https://doi.org/10.2307/258191
16. FATF (2023), *Money Laundering and Terrorist Financing Risks and Trends*, Financial Action Task Force, Paris. Available at: https://www.fatf-gafi.org/ (Accessed 15 May 2026).
17. Hayes, R., Wallage, P. and Gortemaker, H. (2020), *Principles of Auditing: An Introduction to International Standards on Auditing*, 4th ed., Pearson, Harlow.
18. Hopwood, W.S., Leiner, J.J. and Young, G.R. (2012), *Forensic Accounting and Fraud Examination*, 2nd ed., McGraw-Hill, New York.
19. IMF (2024), *Zimbabwe: Staff Report and Economic Outlook*, International Monetary Fund, Washington, DC. Available at: https://www.imf.org/ (Accessed 15 May 2026).
20. Jensen, M.C. and Meckling, W.H. (1976), "Theory of the firm: Managerial behavior, agency costs and ownership structure", *Journal of Financial Economics*, Vol. 3 No. 4, pp. 305–360. https://doi.org/10.1016/0304-405X(76)90026-X
21. Kassem, R. and Higson, A.W. (2021), "External auditors and corporate corruption: Implications for fraud governance and forensic accounting", *Journal of Financial Crime*, Vol. 28 No. 2, pp. 455–472. https://doi.org/10.1108/JFC-01-2020-0013
22. Knechel, W.R. and Salterio, S.E. (2016), *Auditing: Assurance and Risk*, 4th ed., Routledge, London.
23. Levi, M. and Reuter, P. (2006), "Money laundering", *Crime and Justice*, Vol. 34 No. 1, pp. 289–375. https://doi.org/10.1086/501508
24. Lincoln, Y.S. and Guba, E.G. (1985), *Naturalistic Inquiry*, Sage, Beverly Hills.
25. Manning, G.A. (2019), *Financial Investigation and Forensic Accounting*, 3rd ed., CRC Press, Boca Raton.
26. Messier, W.F., Glover, S.M. and Prawitt, D.F. (2017), *Auditing and Assurance Services*, 10th ed., McGraw-Hill, New York.
27. Mhlanga, D. (2024), "FinTech, digital transformation and cyber-risk in Zimbabwe's banking sector", *African Journal of Economic and Management Studies*, Vol. 15 No. 1, pp. 44–61. https://doi.org/10.1108/AJEMS-03-2023-0117
28. Murphy, P.R. and Free, C. (2021), "Broadening the fraud triangle: Instrumental climate and fraud", *Accounting, Organizations and Society*, Vol. 91, 101190. https://doi.org/10.1016/j.aos.2021.101190
29. Njanike, K. and Mashayanye, E. (2023), "Governance failures and fraud exposure in Zimbabwean banking institutions", *African Journal of Business Management*, Vol. 17 No. 2, pp. 78–96.
30. Ozili, P.K. (2020), "The impact of digital finance on financial inclusion and banking stability", *Borsa Istanbul Review*, Vol. 20 No. 4, pp. 329–340. https://doi.org/10.1016/j.bir.2020.05.003
31. PwC (2022), *Global Economic Crime and Fraud Survey 2022*, PricewaterhouseCoopers, London. Available at: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (Accessed 15 May 2026).
32. Reserve Bank of Zimbabwe (2023), *Monetary Policy Statement*, RBZ, Harare. Available at: https://www.rbz.co.zw/ (Accessed 15 May 2026).
33. Rezaee, Z. and Riley, R. (2019), *Financial Statement Fraud: Prevention and Detection*, 3rd ed., Wiley, Hoboken.
34. Rezaee, Z. and Wang, J. (2019), *Relevance of Accounting and Auditing in Fraud Detection and Governance*, Wiley, Hoboken.

35. Singleton, T.W. and Singleton, A.J. (2010), *Fraud Auditing and Forensic Accounting*, 4th ed., Wiley, Hoboken.
36. Solomon, J. (2021), *Corporate Governance and Accountability*, 5th ed., Wiley, Hoboken.
37. Saunders, M., Lewis, P. and Thornhill, A. (2019), *Research Methods for Business Students*, 8th ed., Pearson, Harlow.
38. Snyder, H. (2019), "Literature review as a research methodology: An overview and guidelines", *Journal of Business Research*, Vol. 104, pp. 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
39. Thomas, J. and Harden, A. (2008), "Methods for the thematic synthesis of qualitative research in systematic reviews", *BMC Medical Research Methodology*, Vol. 8 No. 45.https://doi.org/10.1186/1471-2288-8-45
40. Torraco, R.J. (2016), "Writing integrative literature reviews", *Human Resource Development Review*, Vol. 15 No. 4, pp. 404–428. https://doi.org/10.1177/1534484316671606
41. Treviño, L.K., Weaver, G.R. and Reynolds, S.J. (2006), "Behavioral ethics in organizations", *Journal of Management*, Vol. 32 No. 6, pp. 951–990. https://doi.org/10.1177/0149206306294258
42. UNECA (2020), *Economic Development in Africa Report: Tackling Illicit Financial Flows*, United Nations Economic Commission for Africa, Addis Ababa. Available at: https://www.uneca.org/ (Accessed 15 May 2026).
43. Van Graan, C., Roos, V. and Katjene, M. (2024), "Forensic interviewing and evidence reliability in financial investigations", *Journal of Financial Crime*, Vol. 31 No. 1, pp. 90–109. https://doi.org/10.1108/JFC-05-2023-0108
44. Vona, L.W. (2020), *Fraud Data Analytics Methodology*, Wiley, Hoboken.
45. Wolfe, D.T. and Hermanson, D.R. (2004), "The fraud diamond: Considering the four elements of fraud", *CPA Journal*, Vol. 74 No. 12, pp. 38–42.
46. World Bank (2023), *Zimbabwe Economic Update: Unlocking Sustainable Growth*, World Bank, Washington, DC. Available at: https://www.worldbank.org/ (Accessed 15 May 2026).
47. Yar, M. (2005), "The novelty of cybercrime: An assessment in light of routine activity theory", *European Journal of Criminology*, Vol. 2 No. 4, pp. 407–427. https://doi.org/10.1177/147737080556056