

Adoption of Forensic Accounting Techniques and Contemporary Fraud Detection Mechanisms in the Financial Sector in Zimbabwe

Severino Mashiri¹, David Chisunga²

^{1,2}Department of Forensic Accounting and Auditing, School of Business and Management Sciences, Harare Institute of Technology, Harare, Zimbabwe

Abstract:

Zimbabwe's financial sector faces a sophisticated wave of financial crime that outpaces traditional compliance-driven, paper-based oversight. This study examines the incorporation of forensic accounting techniques in registered commercial banks and insurance companies in Harare, investigating the gap between formal adoption and practical, real-time day-to-day application. Grounded in Fraud Diamond Theory, Differential Association Theory, and Institutional Theory, the study explains individual drivers of fraud alongside institutional performance dynamics. A sequential explanatory mixed-methods design was employed. Quantitative questionnaires were gathered from 100 purposively selected oversight professionals and analyzed using SPSS, followed by ten semi-structured thematic interviews analyzed via NVivo. Findings show an industry formally compliant but operationally under-equipped: 92% of institutions remain reliant on compliance checklists, 64% report no predictive analytics, and 72% lack continuous digital surveillance. However, data mining adoption strongly correlates with fraud detection effectiveness (Pearson $r = 0.742$, $p < .01$), and machine learning accounts for 61% of financial loss reduction variance. Structural barriers include legacy system incompatibility (68%), prohibitively expensive foreign licensing costs, and an entrenched tick-box culture (82%). A decoupling effect exists where compliance satisfies regulatory mandates on paper while departments remain operationally under-resourced. Compulsory forensic readiness audits and API-integrated systems are recommended.

Keywords: Forensic Accounting, Fraud Detection, Data Mining, Machine Learning, Capability Gap

Introduction

The financial sector serves as the core of any developing economy. However, the swelling proliferation of complex financial crimes continue to challenge systemic stability. Traditional auditing methodologies often prove inadequate to detect intricately moulded, technologically enabled fraudulent transactions. This structural vacuum allows forensic accounting to become an essential, specialized practice worldwide, merging advanced investigative methods with core accounting principles to bridge gaps in financial crime detection.

The financial landscape has been fundamentally transformed over the past two decades by the exponential growth of digital finance technologies, international capital movements, and ever-evolving corporate governance systems. Traditional auditing approaches, developed primarily to ensure statutory compliance and retrospective historical accuracy, look backward through "the rearview mirror".

Conversely, contemporary fraud syndicates operate dynamically, using real-time and algorithmic financial manipulation. This creates an expanding audit expectation gap—the discrepancy between what auditors deliver and what stakeholders expect regarding active fraud discovery.

Within the Southern African Development Community (SADC) and specifically Zimbabwe, mobile money and decentralized fintech have expanded financial inclusion while opening new avenues for cyber-fraud, cross-border laundering, and electronic embezzlement. Macroeconomic factors such as hyperinflation, currency devaluation, and intense fiscal volatility systematically enhance financial pressure on potential perpetrators. Despite the academic consolidation of forensic accounting as an effective tool, sophisticated tools remain in their infancy and unevenly distributed in local commercial banking and insurance ecosystems. This study addresses the capability gap across the Zimbabwean financial sector by presenting original empirical data evaluating adoption status, operational barriers, and institutional dynamics.

Literature Review

Theoretical Framework

Fraud Diamond Theory

The Fraud Diamond Theory expands Cressey's classical Fraud Triangle by introducing a fourth element: Capability. In a digital banking context, financial pressure and organizational opportunities are insufficient on their own; high-level electronic fraud requires technical capacity and a position of authority to execute successfully. This capability combines advanced IT literacy, privileged information access, and hierarchical clout to deliberately bypass institutional safeguards. Sophisticated criminals exploit the geographical and temporal limitations of outdated compliance software. A structural knowledge asymmetry occurs when the capabilities of internal auditors are lower than those of technically advanced perpetrators.

Differential Association Theory

Sutherland's Differential Association Theory posits that white-collar financial crime is a learned social response propagated through intimate interactions within occupational and institutional environments. Employees surrounded by workplace subcultures that condone financial shortcuts, creative accounting, or management overrides internalize favorable definitions of rule-breaking. Group-level collusion allows multiple actors to collaborate in altering bank ledgers and circumventing standard internal review procedures, especially where the general ethical climate is weak.

Institutional Theory

Institutional Theory explains that organizations subjected to external regulatory coercion often implement structures and formal policies primarily to secure external stakeholder legitimacy, regardless of whether those tools improve operational performance. This coercive isomorphism leads financial institutions to establish compliance units and write extensive anti-fraud policies to satisfy central bank requirements. However, this response frequently results in regulatory "decoupling," where an organization maintains an extensive paper trail but deliberately under-resources the data mining software, technical systems integration, and professional staff required for real-time digital surveillance.

Conceptual Architecture

The conceptual framework maps the Capability Gap—the structural mismatch between modern financial crime sophistication and established control environments. This gap is driven by three tiers of determinants: individual-level factors (technical capability and normalized social learning), institutional-

level factors (legacy architectures, cost-center resource cuts, and restrictive corporate cultures), and macro-environmental factors (macroeconomic volatility and regulatory compliance demands). Forensic tools, including predictive data mining, continuous surveillance, and mathematical anomaly detection, serve as mediating mechanisms determining overall fraud detection efficacy.

Research Methodology

This investigation adopted a sequential explanatory mixed-methods research design. The initial phase comprised quantitative data collection and analysis to establish statistical patterns. This was followed by a qualitative phase using semi-structured interviews to explain, contextualize, and enrich the quantitative findings. Grounded in a pragmatist philosophy, this methodology emphasizes practical, applied research problem-solving by selecting tools that best address the multi-dimensional empirical questions.

The target population comprised 133 senior financial monitoring and oversight officers across registered commercial banks and highly capitalized insurance firms in Harare, Zimbabwe. This focused community included four specific professional categories with the mandatory expertise and institutional access to evaluate forensic adoption: forensic accountants, internal auditors, compliance and risk officers, and IT security specialists. General branch staff were excluded. Based on the Yamane formula at a 95% confidence level, the required sample size was calculated as 100 participants. Non-probability purposive sampling was used to ensure proportional representation across professional divisions.

Quantitative data were gathered using a structured questionnaire, using a four-point scale for tracking tool usage frequency and a five-point Likert scale to measure barrier severity. Qualitative information was obtained from ten senior managers via semi-structured interview guides containing open-ended queries and analytical probes. Face and content validity were verified by academic experts from the Department of Forensic Accounting and Auditing. Reliability was pre-tested using pilot studies, yielding a acceptable Cronbach's alpha (0.70). SPSS was used for descriptive frequencies, Pearson correlations, linear regressions, and t-tests. NVivo supported qualitative thematic coding, allowing data integration through systematic triangulation.

Data Analysis and Presentation

Demographic and Capability Baseline

The study achieved a 100% response rate across both phases. The multidisciplinary sample consisted of internal auditors (34%), compliance and risk officers (28%), forensic accountants (19%), and IT security specialists (19%). This distribution shows that the sector remains structurally geared toward traditional compliance management rather than dedicated forensic investigation. Long-term professional experience was well represented, with 88% of respondents holding over five years of active oversight experience and 46% exceeding ten years.

A key structural aspect of the capability gap appears in professional qualifications: 94% of respondents hold postgraduate or certified professional credentials, but only 22% possess forensic-specific certifications such as Certified Fraud Examiner (CFE) or Certified Information Systems Auditor (CISA). The majority (48%) hold traditional accounting certifications lacking specialized training in data science, forensic data mining, or digital analytics.

Quantitative Findings on Tool Integration and Efficacy

Descriptive statistics reveal a heavily compliance-reliant, operationally under-equipped control environment. Statutory compliance checklists remain the principal fraud-control mechanism for 92% of

institutions. Conversely, 64% of respondents report limited or no usage of predictive analytics, and 72% indicate a complete absence of continuous digital surveillance capabilities.

Where advanced techniques have been deployed, they demonstrate clear operational utility. Pearson correlation analysis reveals a strong, positive, and statistically significant relationship between the adoption of predictive data mining techniques and overall fraud detection effectiveness ($r = .742$, $p < .01$). Furthermore, linear regression testing confirms that machine learning deployment serves as a strong predictor of loss mitigation, accounting for 61% of the total variance in financial loss reductions within those institutions ($R^2 = .61$).

Structural Barriers and the Decoupling Phenomenon

The empirical results identify significant barriers to full forensic technology operationalization across three primary dimensions: technical, financial, and cultural. Legacy core banking system incompatibility was cited by 68% of respondents as a critical technical barrier preventing seamless data migration and integration with modern AI-driven forensic architectures. Financially, the US dollar-denominated licensing fees for international forensic software create a major barrier under conditions of intense macroeconomic volatility and foreign currency scarcity, scoring a weighted mean of 4.82 out of 5. Culturally, an entrenched tick-box compliance mindset was identified by 82% of respondents as a key institutional barrier to genuine capability building.

These findings confirm the regulatory decoupling hypothesis. Financial institutions actively maintain extensive formal policy documentation and structural frameworks to fulfill the coercive requirements of the Reserve Bank of Zimbabwe. However, qualitative thematic triangulation reveals that these measures are often performative. Operational forensic accounting departments remain structurally under-resourced, technologically isolated, and under-equipped to execute proactive, real-time digital fraud containment.

Table and Figure Overviews

Table 1: Targeted Professional Sample Distribution (n=100)

Category	Targeted Population	Active Sample Size	Sample Percentage
Internal Auditors	45	34	34.0%
Compliance and Risk Officers	38	28	28.0%
Forensic Accountants	25	19	19.0%
IT Security Specialists	25	19	19.0%
Total	133	100	100.0%

(Source: Primary Research Data, compiled via SPSS)

Table 2: Statistical Predictive Metrics Matrix

Core Variable	Predictive	Pearson Correlation (r)	Significance Level (p)	Variance Explained (\$R^2\$)
Data Mining Adoption		.742	$p < .01$	—
Machine Learning Toolsets		—	$p < .01$	61.0%

(Source: Primary Empirical Output, extracted via SPSS Regression Models)

Discussion and Conclusion

The empirical evidence indicates that the capability gap across Zimbabwe's financial sector is structural rather than accidental. While financial institutions demonstrate high formal compliance with central bank directives, their practical operational frameworks are inadequate against sophisticated digital fraud typologies. The systemic decoupling phenomenon allows organizations to secure external regulatory legitimacy via extensive policy documentation while remaining exposed to real-time losses. This dynamic confirms Institutional Theory: the symbolic apparatus of compliance is prioritized over digital data mining tools, system interoperability, and specialized human capital.

When deployed, however, advanced forensic tools show clear utility. The strong correlation between predictive data mining and detection efficacy ($r = .742$), combined with the 61% loss reduction variance explained by machine learning, demonstrates that transition to algorithmic monitoring provides measurable defensive value. Resolving the capability gap requires addressing the key structural barriers identified, particularly legacy system incompatibility, high foreign licensing costs, and a tick-box compliance culture.

Ultimately, moving beyond performative regulatory compliance requires a strategic shift from retrospective checklist tracking toward proactive, technology-enabled forensic monitoring. Mitigating these vulnerabilities requires structural updates to core software infrastructures, localized software development to reduce foreign currency licensing dependence, and professional upskilling to blend traditional accounting with forensic data science.

References

1. Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2018). *Fraud examination* (6th ed.). Cengage Learning.
2. Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud analytics using descriptive, predictive, and social network analytics: A guide to data science for fraud detection*. John Wiley & Sons.
3. Bhasin, M. L. (2016). Forensic accounting in the cyber-world: A study of its introduction, tools, and importance. *International Journal of Contemporary Business Studies*, 7(2), 34– 49.
4. Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
5. Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

6. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147– 160.
7. Dzomira, S. (2015). Electronic fraud detection and the capability gap in the banking sector in Zimbabwe. *Journal of Forensic and Investigative Accounting*, 7(1), 112– 134.
8. Elemide, O. A., & Araoye, F. E. (2024). Artificial intelligence and machine learning applications in forensic accounting: A systematic review. *Journal of Financial Crime*, 31(1), 78– 95.
9. Goswami, R. (2021). Institutional theory and regulatory decoupling in financial risk architectures. *Journal of Business Research*, 129(3), 412– 425.
10. Kranacher, M. J., & Riley, R. (2019). *Forensic accounting and fraud examination* (2nd ed.). John Wiley & Sons.
11. Lokanan, M. E. (2015). Using Sutherland's differential association theory to explain white-collar financial crimes. *Journal of Financial Crime*, 22(4), 430– 446.
12. Magombedze, A., & Gunduza, C. (2018). The impact of forensic accounting on corporate fraud deterrence in emerging economies: Empirical evidence from Zimbabwe. *African Journal of Accounting and Finance*, 4(2), 56– 72.
13. Perols, J. L., Bowen, R. M., Evans, C., & Hardin, J. R. (2017). Finding financial statement fraud using machine learning algorithm models. *Journal of Information Systems*, 31(2), 19– 39.
14. Sharma, A., & Panigrahi, P. K. (2020). A review of data mining and machine learning techniques in financial fraud detection. *International Journal of Computer Applications*, 174(12), 22– 31.
15. Suh, J. B., Nicolaides, R., & Trafford, R. (2019). Internal controls and management override in international banking frauds. *Journal of Financial Regulation and Compliance*, 27(4), 488– 502.
16. Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal*, 74(12), 38– 42.
17. Zhou, L., Mazhambe, A., & Njaya, T. (2020). Social learning dynamics and normalized misconduct in local authorities: A case study of Masvingo Province. *Zimbabwe Journal of Technological Sciences*, 8(1), 45– 61.