The Effectiveness of Flagging Systems in Detecting Fraud among Registered Micro-Finance Institutions in Lusaka, Zambia

Liyungu Imalimbila[1], Dr Bwalya Chilolo[2]

[1]School of Business, University of Zambia, Zambia

[2]Lecturer, University of Zambia, Zambia

DOI: https://doi.org/10.47772/IJRISS.2026.100400238

Received: 16 April 2026; Accepted: 22 April 2026; Published: 05 May 2026

ABSTRACT

This study investigated the effectiveness of flagging systems in detecting fraud among registered microfinance institutions in Lusaka. Microfinance institutions play a critical role in promoting financial inclusion; however, persistent fraud and high non-performing loans suggest weaknesses in existing detection mechanisms. The study aimed to determine the standard flagging systems used, assess their effectiveness, and examine the challenges affecting their performance. A pragmatic research philosophy was adopted, utilising a mixed research approach. A cross-sectional survey design was employed, with primary data collected from 108 employees across two microfinance institutions using structured questionnaires and semi structured interviews. Quantitative data were analysed using SPSS through descriptive and inferential statistics, while qualitative data were analysed thematically to provide contextual insights. The findings revealed that institutions relied on a hybrid system combining integrated core banking modules, manual processes, and limited advanced technologies. Flagging systems contributed to fraud detection, although effectiveness was generally moderate, with inconsistencies in detection speed, accuracy, and fraud reduction outcomes. The regression analysis further showed that the model was statistically significant ($F = 5.232$, $p = 0.000$) and explained 23.70 percent of the variation in fraud detection effectiveness. Reliance on automated digital flagging systems had a significant positive effect on effectiveness ($B = 0.126$, $p = 0.004$), while technical system limitations had a significant negative effect ($B = -0.131$, $p = 0.004$). Formal training also had a significant positive influence ($B = 0.085$, $p = 0.048$), while other variables such as system interaction frequency, perceived training insufficiency, and policy constraints showed weaker or insignificant effects. Key challenges identified included system limitations, poor data quality, insufficient staff training, false alerts, and institutional constraints. The results indicated that while flagging systems improved fraud detection, their effectiveness was strongly shaped by technology quality, automation, and staff capacity. The study concluded that although flagging systems enhance fraud detection, their effectiveness is constrained by technological and operational factors. The study recommends system integration, adoption of advanced technologies, regular system updates, improved data management, and continuous staff training to strengthen fraud detection and institutional resilience.

INTRODUCTION

Flagging systems, in general terms, are structured mechanisms designed to identify unusual, irregular, or potentially harmful activities within a system or process (Arnold & Wade, 2015). They operate by continuously monitoring behaviours, events, or data flows and comparing them against predefined norms, rules, or expected patterns. When deviations occur, the system generates alerts or “flags” to signal the need for further investigation or corrective action (Kunc, 2024). Such systems are widely applied across sectors including healthcare, cybersecurity, manufacturing, education, and governance, where early detection of anomalies is essential for effective risk management and decision-making (Sutton, Pincock, & Baumgart, 2020). In the financial sector, flagging systems are specifically used to monitor transactions, customer activities, and internal processes to detect fraud, errors, or compliance violations (Hilal, Gadsden, & , 2022). Financial institutions rely on these systems to analyse large volumes of transactional data either in real time or periodically, using predefined rules, thresholds, and analytical models to identify suspicious patterns (Olufemi,

Bello, & Olufemi, 2024). Common indicators include unusually large or frequent transactions, inconsistent account activity, abnormal loan disbursement trends, and deviations from expected behavioural profiles of customers or staff. Once anomalies are detected, alerts are generated for review by compliance, audit, or risk management teams.

In Zambia, microfinance institutions (MFIs) have expanded significantly over the past two decades, largely driven by efforts to enhance financial inclusion among low-income households, micro-entrepreneurs, and small businesses excluded from traditional banking systems (Sichuundu, 2024). This growth has been supported by regulatory reforms, rising demand for microcredit, and policy initiatives aimed at poverty reduction and economic empowerment (Paliyani & Silwimba, 2025). Consequently, MFIs have become an important part of Zambia's financial landscape, particularly in urban areas such as Lusaka, where informal economic activity is concentrated (Kalunga, 2017).

Despite these benefits, the rapid growth of microfinance has increased exposure to financial fraud risks. Compared to conventional banks, MFIs typically employ flexible lending procedures, simplified documentation, and faster loan approvals (Dolo, 2025). While these features improve access to finance, they also create vulnerabilities that can be exploited. Factors such as limited collateral requirements, group lending models, and high transaction volumes complicate effective monitoring and heighten fraud risk.

Fraud in MFIs can occur through multiple channels, including loan application fraud, where clients provide false information or use multiple identities; insider fraud, involving staff manipulation of records or diversion of funds; and repayment fraud, such as misreporting of collections (Pebruary & Edward, 2019). Additional risks arise from digital platforms, including mobile money and online registration systems, where weak controls may enable identity misuse or transaction manipulation. Other forms include ghost borrowers, inflated loan portfolios, and collusion between staff and clients. Although flagging systems are increasingly adopted, fraud and credit risks remain persistent in Zambia. Data from the Bank of Zambia indicate ongoing challenges in loan performance, suggesting weaknesses in risk detection and control mechanisms (Funyina & Muhanga, 2021). Between 2011 and 2018, non-performing loan (NPL) rates frequently exceeded the 10% prudential threshold. For instance, NPLs stood at 14% in January 2011, declined slightly, but fluctuated and rose again to 13% by January 2018 (Chibawe & Haabazoka, 2025; Arhinful & Mensah, 2025; Mahlangu & Chowa, 2022). Although there was a period of relative stability between 2012 and 2016, the upward trend resumed thereafter.

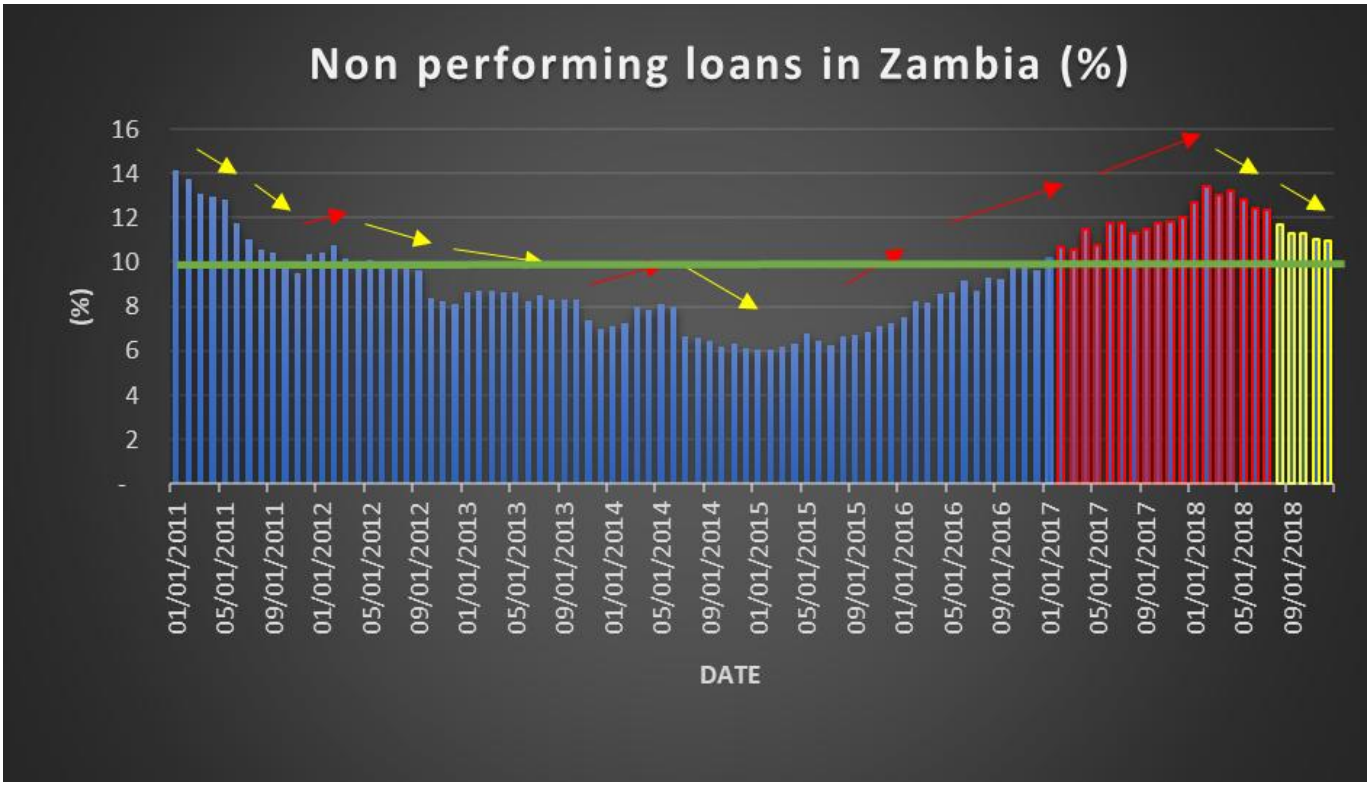

Figure 1. Monthly Data on Non-Performing Loans (NPLs) in Zambia

These patterns indicate that the mere presence of flagging systems is insufficient to curb fraud. Persistent weaknesses highlight the need to evaluate their effectiveness, design, and implementation. Therefore, this study is justified in assessing how effectively flagging systems detect fraud in Lusaka's MFIs, with the aim of strengthening internal controls, informing policy, and improving sector stability.

Research problem

Microfinance institutions (MFIs) in Zambia have become vital in promoting financial inclusion, particularly among low-income households and micro-entrepreneurs who are often excluded from formal banking systems (Sichuundu, 2024; Paliyani & Silwimba, 2025). Theory suggests that the adoption of structured monitoring mechanisms, such as flagging systems, should enable MFIs to detect and prevent fraudulent activities effectively (Arnold & Wade, 2015; Kunc, 2024). These systems are expected to monitor transactions, compare them against predefined norms, and generate alerts when anomalies occur, thereby reducing financial losses and enhancing institutional stability (Hilal, Gadsden, & , 2022; Olufemi, Bello, & Olufemi, 2024). In practice, however, the continued prevalence of fraud and high non-performing loans (NPLs) among MFIs in Lusaka indicates a divergence from these theoretical expectations. Data from the Bank of Zambia show that NPLs frequently exceeded the prudential threshold of 10% between 2011 and 2018, reaching 14% at the start of 2011 and fluctuating above the regulatory limit in subsequent years (Chibawe & Haabazoka, 2025; Arhinful & Mensah, 2025; Mahlangu & Chowa, 2022). These statistics suggest that, despite the presence of flagging systems, the mechanisms in place may be insufficient, poorly implemented, or inadequately utilised to curb fraud effectively.

The persistence of fraud-related risks raises significant concerns for MFIs' sustainability, credibility, and contribution to economic development. Failure to address these challenges threatens not only institutional financial stability but also the livelihoods of clients, particularly micro-entrepreneurs who depend on timely and secure access to credit. Additionally, systemic fraud undermines regulatory compliance and can create ripple effects across the broader financial sector, weakening public trust and discouraging investment.

Prior studies have addressed fraud detection and control measures but exhibit notable gaps. Mubita (2023) and Agubata (2022) examined general controls and red flags in contexts outside Lusaka or mobile money systems, while Yucel (2020), Tonui, Kamau, and Ombui (2018), and Musyoki (2023) focused on internal controls and auditors' perceptions without empirically assessing real-time flagging system effectiveness in MFIs. Similarly, Nyirenda (2024) and Taranhike and Bwalya (2025) explored MFI success factors and SME financing, leaving fraud detection mechanisms largely unexplored. This study addresses these gaps by empirically investigating the types, effectiveness, and operational challenges of flagging systems in detecting fraud among registered MFIs in Lusaka, providing actionable insights to strengthen internal controls, policy, and institutional resilience.

Significance, objectives and scope of the study

The significance of this study is anchored in its aim to determine the effectiveness of flagging systems in detecting fraud among microfinance institutions in Lusaka, Zambia. The purpose is to develop a clear understanding of how these systems function in practice, evaluate their ability to identify and prevent fraudulent activities, and examine the challenges that limit their performance. The study is guided by key research questions which seek to establish the types of flagging systems used, assess how effective they are, and identify the challenges faced during their use. These questions are supported by specific objectives that focus on identifying standard systems, evaluating their effectiveness, and investigating operational constraints, thereby addressing the gap between theoretical expectations and practical outcomes (Arnold and Wade, 2015; Kunc, 2024).

This study is practically significant to several stakeholders. Management of microfinance institutions can use the findings to strengthen internal control systems and reduce fraud related losses. Regulators such as the Bank of Zambia may benefit by using the evidence to improve regulatory policies and supervision mechanisms. Investors and donors can gain confidence through improved transparency and reduced financial risk, while clients benefit from more secure and reliable financial services. Employees within institutions may also use the findings to improve compliance practices and operational efficiency.

In terms of empirical contribution, the study addresses gaps in existing literature which has largely focused on general fraud controls or contexts outside Lusaka (Mubita, 2023; Agubata, 2022; Yucel, 2020). It provides context specific evidence on the effectiveness of flagging systems in microfinance institutions.

The scope of the study is limited to registered microfinance institutions in Lusaka District and focuses specifically on fraud detection through flagging systems, their effectiveness, and the challenges associated with their implementation.

LITERATURE REVIEW

Theoretical Literature

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed the COSO Framework in 1992 as a comprehensive model for designing, implementing, and evaluating internal control systems within organizations (Teresa , 2024). The framework was originally developed by a coalition of five private-sector organizations in the United States with the primary aim of improving organizational performance and governance, mitigating the risk of financial reporting fraud, and restoring public confidence following high-profile corporate scandals in the 1980s and early 1990s (Renes, 2000). COSO provides an integrated approach to internal controls by defining a set of principles and components that enable organizations to achieve objectives related to operations, financial reporting, and compliance while managing risks effectively (Figure 2).

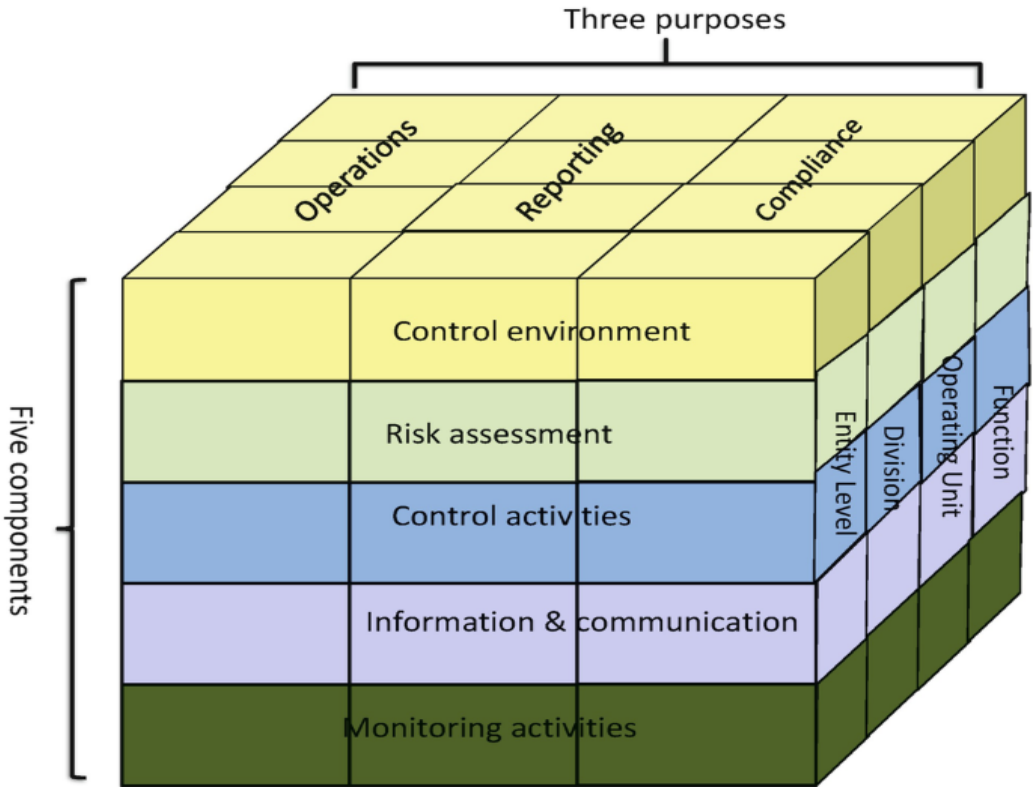

Figure 2. COSO Framework

The COSO Framework consists of five interrelated components: control environment, risk assessment, control activities, information and communication, and monitoring activities. The control environment represents the foundation of internal control and encompasses organizational culture, ethical values, management integrity, and governance structures. Risk assessment involves identifying and analysing risks that may prevent the achievement of objectives, including fraud risks (Chowdhury, 2025). Control activities refer to the policies, procedures, and practices established to mitigate identified risks. Information and communication ensure that relevant data is captured and communicated promptly for decision-making, while monitoring activities involve ongoing or periodic evaluations to ensure that controls are operating effectively (Lyons, 2012). Together, these components create a cohesive system that allows organizations to detect, prevent, and respond to fraud and other operational risks (see Figure 2).

In the context of this study, the COSO Framework provides a theoretical foundation for investigating the effectiveness of flagging systems in detecting fraud within microfinance institutions (MFIs) in Lusaka, Zambia. The framework is particularly relevant because flagging systems function as internal control mechanisms that identify unusual or suspicious financial transactions, thereby enhancing organizational oversight and risk mitigation. Among the COSO components, this study focuses on those most applicable to fraud detection through flagging systems. The control environment is critical, as it shapes the ethical standards and commitment to transparency among MFI staff, influencing how effectively alerts generated by flagging systems are acted upon. Risk assessment is equally important, as it allows institutions to identify areas most vulnerable to fraud, such as loan disbursement or digital payment channels, and tailor flagging parameters accordingly. Control activities directly relate to the operational use of flagging systems, including transaction monitoring, verification procedures, and automated alert generation. Finally, information and communication are central, as accurate and timely reporting of flagged anomalies ensures that management and audit personnel can respond promptly to potential fraud (see Figure 2).

Based on these applied COSO dimensions, the study identifies four independent variables that can be empirically examined in relation to the dependent variable, flagging system fraud detection within Lusaka-based MFIs. These include: (1) the strength of the control environment, measured by staff adherence to ethical standards and management commitment; (2) risk assessment practices, evaluated by the thoroughness of fraud risk identification and prioritization; (3) effectiveness of control activities, captured through the operational efficiency of flagging systems, transaction monitoring, and verification procedures; and (4) information and communication quality, assessed by the timeliness and reliability of reporting flagged incidents to relevant personnel.

Applying the COSO Framework in this context allows the study to systematically examine how internal control components influence the functionality and effectiveness of flagging systems, addressing the objectives of determining standard systems, assessing their effectiveness, and identifying operational challenges in Lusaka's microfinance sector. By linking theory to practice, the framework provides a structured lens to understand both organizational and technological factors affecting fraud detection, while offering actionable insights for strengthening institutional controls (see Figure 2).

Empirical Literature

The reviewed literature provides extensive empirical evidence on fraud detection, control mechanisms, and operational challenges within financial institutions, particularly microfinance institutions and related sectors. Mubita (2023) examined the adequacy of control measures in combating mobile money fraud in Lusaka using a mixed methods approach. The study found that while measures such as user sensitisation, prosecution of offenders, and technological safeguards were in place, their effectiveness was limited by low user compliance and inadequate awareness of existing policies. This highlights the gap between the availability of controls and their actual utilisation.

Similarly, Agubata (2022) investigated the role of red flags in fraud detection in microfinance banks and found that structural, financial, and operational red flags significantly improved fraud detection, while personnel related red flags had an inverse effect. The study emphasised the importance of strengthening internal systems and recommended whistle blowing mechanisms. In a related context, Yucel (2020) found that red flags were generally only somewhat effective in detecting fraudulent financial reporting, although opportunity related indicators were more impactful, suggesting that fraud risks are strongly linked to systemic vulnerabilities.

Tonui, Kamau, and Ombui (2018) explored forensic accounting in microfinance institutions and revealed mixed results, where internal controls and technology showed negative relationships with fraud detection, while the control environment had a positive influence. This suggests that the effectiveness of controls depends on how they are implemented. Nyirenda (2024) identified broader institutional challenges in Lusaka, including limited funding, low efficiency, and poor financial literacy, which affect the sustainability of microfinance institutions.

Musyoki (2023) and Yolanda (2013) both emphasised the critical role of strong internal control systems in fraud prevention. Their findings highlighted that effective monitoring, ethical practices, and regular system updates are essential in reducing fraud opportunities. Boateng, Boateng, and Acquah (2020) further identified systemic issues

such as weak governance, corruption, and inadequate regulatory oversight as key contributors to fraud in microfinance institutions.

Additionally, Taranhike and Bwalya (2025) and Ramadhany (2025) highlighted operational and human factors, including restrictive lending conditions and the importance of auditor competence, awareness, and professional skepticism in enhancing fraud detection. Therefore, the literature reveals that while various fraud detection mechanisms exist, their effectiveness is often constrained by poor implementation, weak institutional capacity, and human factors, thereby justifying further empirical investigation.

Literature Gaps

The reviewed literature reveals several important gaps in understanding fraud detection mechanisms within microfinance institutions, particularly in the context of Lusaka, Zambia. Mubita (2023) examined general control measures for mobile money fraud, such as user sensitisation and technological safeguards, but did not focus on flagging systems as institutional tools for detecting fraud. The study also highlighted low compliance among users, indicating limited effectiveness of existing measures. Similarly, Agubata (2022) explored red flags in fraud detection but was limited to a different geographical context and did not consider institutional or environmental factors affecting their effectiveness in Zambia.

Yucel (2020) provided theoretical insights into red flags in financial reporting but relied on auditor perceptions rather than actual detection outcomes and did not address microfinance settings. Tonui, Kamau, and Ombui (2018) focused on forensic accounting and internal controls in Kenya without specifically analysing flagging systems or their implementation challenges. Nyirenda (2024) examined success and failure factors of MFIs in Lusaka but did not consider fraud detection mechanisms, leaving a gap in understanding operational safeguards.

Further gaps are evident in studies such as Musyoki (2023) and Yolanda (2013), which broadly addressed internal controls without isolating flagging systems as distinct fraud detection tools. Taranhike and Bwalya (2025) focused on financial service delivery and SME performance, while Ramadhany (2025) examined auditor behaviour in commercial banks, both overlooking practical applications of flagging systems in MFIs. Boateng, Boateng, and Acquah (2020) also provided theoretical insights but lacked empirical analysis of detection systems.

Therefore, the literature is limited by its focus on other sectors, reliance on perceptions rather than real time data, and lack of contextual relevance to Lusaka. This study addresses these gaps by empirically examining the types, effectiveness, and challenges of flagging systems in Lusaka based MFIs.

Conceptual framework

The conceptual framework of this study is grounded in the principles of the COSO Internal Control Framework, which provides a structured approach to designing, implementing, and evaluating internal controls to mitigate risks, including fraud. Developed in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the framework was designed to help organizations improve performance, ensure reliable reporting, and comply with laws and regulations. COSO identifies five interrelated components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring (COSO, 2013). In the context of microfinance institutions (MFIs), these components guide the selection of internal mechanisms, such as flagging systems, to detect and prevent fraudulent activities. Control activities, in particular, emphasize policies, procedures, and systems designed to detect anomalies, which aligns directly with the use of flagging systems as proactive fraud detection tools. Similarly, risk assessment guides MFIs to identify areas vulnerable to fraud, while monitoring ensures that detection mechanisms remain effective over time (see figure 3).

In this study, the dependent variable is flagging system effectiveness in detecting financial fraud within MFIs in Lusaka. This represents the outcome of interest, reflecting how well microfinance institutions can identify, flag, and respond to suspicious or irregular financial activities. The dependent variable captures real-time operational success in fraud mitigation, aligning with COSO's emphasis on monitoring and control activities (see figure 3).

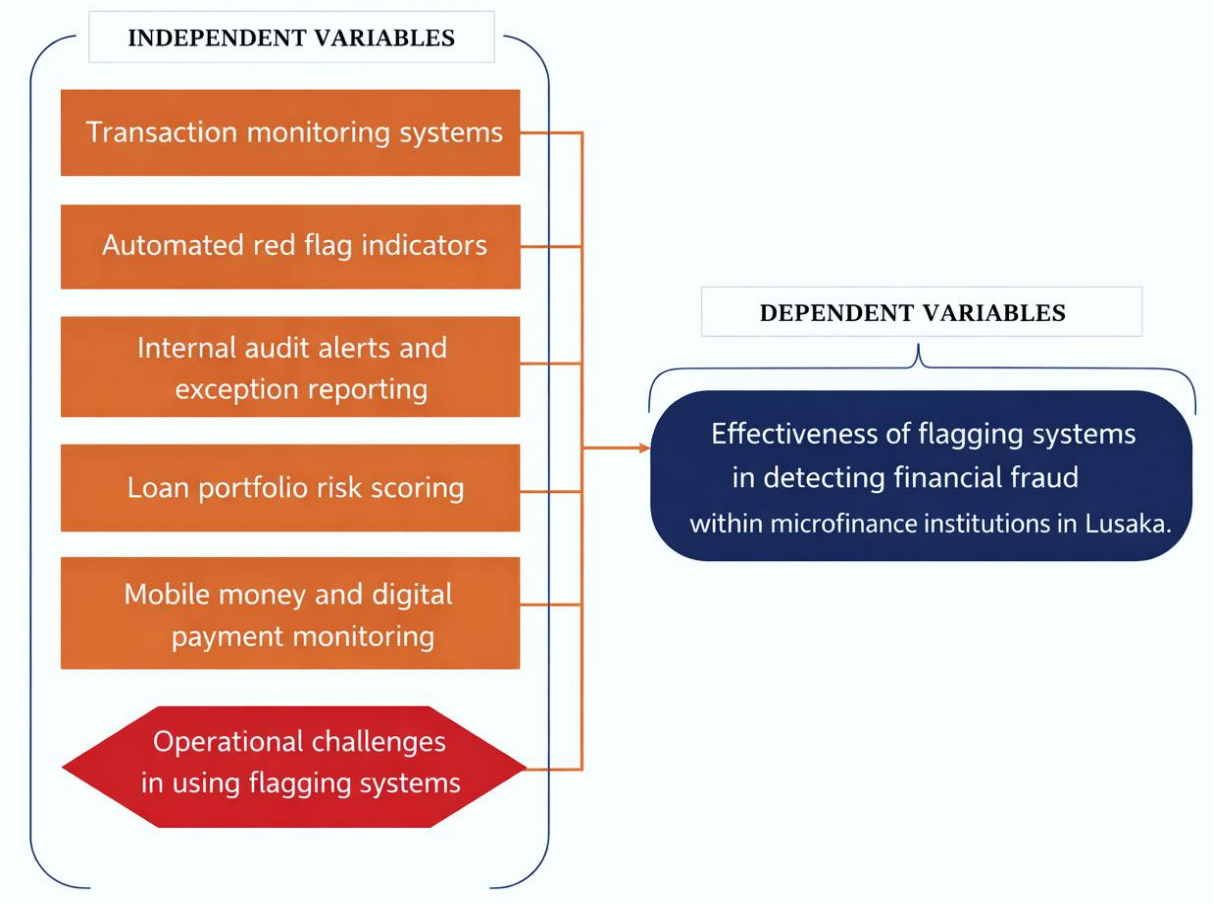

Figure 3. Conceptual framework of the study

METHODOLOGY

The study adopted a pragmatist research philosophy, which enabled the integration of both quantitative and qualitative methods to assess flagging systems in microfinance institutions. This approach was justified by the need to combine objective measurements of system performance, such as alert frequencies and fraud detection rates, with subjective insights from employees regarding operational challenges and contextual factors. A cross sectional survey design was employed to collect primary data at a single point in time, using structured questionnaires for quantitative data and semi structured interview guides for qualitative insights. The mixed methods approach allowed for triangulation, enhancing the credibility and validity of the findings.

The study was conducted in Lusaka, Zambia, targeting employees from two registered microfinance institutions. The population comprised 120 staff members in key operational roles, including credit officers, risk management officers, internal auditors, information technology personnel, and compliance staff. Using Yamane's formula with a five percent margin of error, a sample of 108 employees was selected via stratified random sampling to ensure proportional representation across roles. For the qualitative component, between 15 and 20 participants were purposively selected for semi structured interviews based on their direct involvement and experience with fraud detection systems. Inclusion criteria focused on employees directly engaged in monitoring or managing flagging systems, while those with limited or no interaction with fraud detection processes were excluded.

$$Sample\ size\ (n) = \frac{N}{1 + N(e^2)} = \frac{120}{1 + 120(0.03^2)} = 108.3 = 108\ Employees$$

Data processing involved checking quantitative data for completeness and accuracy, coding categorical responses, and using SPSS software for statistical analysis. Descriptive statistics such as means, percentages, and frequencies were employed, alongside inferential statistics including correlation and regression analysis. Qualitative data from interviews were transcribed and analyzed using thematic content analysis, where

recurring ideas and themes were coded and grouped into categories aligned with the study objectives. Triangulation was applied by combining quantitative findings with qualitative insights to ensure consistency and enhance validity. Validity and reliability were ensured through expert review of instruments, pilot testing with ten employees, and the use of Cronbach's alpha to assess internal consistency. Credibility was strengthened through triangulation and the use of multiple data sources from different employee roles. Trustworthiness was maintained through transparency in the research process, informed consent, confidentiality, and secure data storage. The study was conducted over a period of three to four months.

RESULTS

Demographic analysis

The results indicated that respondents were distributed across three gender categories, with a relatively balanced but slightly heterogeneous composition. The largest proportion of respondents indicated that they preferred not to disclose their gender, accounting for 33.30 percent of the total sample. This was followed by female respondents who constituted 37.00 percent, representing the highest identifiable gender group. Male respondents made up 29.60 percent of the sample, representing the lowest proportion among the disclosed categories. The cumulative distribution showed a steady progression across the three categories, reaching a total of 100 percent of the respondents (Table 1).

Table 1. Gender of respondents

What is the respondent's gender?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	40	37.0	37.0	37.0
	Male	32	29.6	29.6	66.7
	Prefer not to say	36	33.3	33.3	100.0
	Total	108	100.0	100.0	

These findings suggest that there was a considerable level of non-disclosure regarding gender identity, which may reflect privacy concerns or institutional confidentiality preferences among employees in microfinance institutions. However, among those who disclosed their gender, female respondents formed the majority, indicating a relatively strong representation of women in operational and administrative roles within the institutions.

The results revealed that compliance and control officers together with risk management officers each accounted for 19.40 percent of respondents, representing the highest proportions in this category. Other operational staff constituted 16.70 percent, while credit officers, information technology personnel, and internal auditors each accounted for 14.80 percent respectively. This distribution reflected a balanced representation across key operational roles within microfinance institutions (see Figure 4). These findings indicated that the sample included respondents drawn from a broad range of functional departments directly involved in fraud detection and risk management processes. The inclusion of technical, operational, and oversight roles suggested that diverse institutional perspectives on flagging systems were effectively captured. In conclusion, the occupational distribution demonstrated adequate representation of relevant job categories, thereby enhancing the comprehensiveness and reliability of insights on fraud detection systems.

The results further showed that the largest proportion of respondents had 4 to 6 years of experience, accounting for 31.50 percent of the sample. This was followed by those with 7 to 9 years of experience at 21.30 percent and respondents with 10 years and above at 17.60 percent. Individuals with less than 1 year of experience constituted 15.70 percent, while those with 1 to 3 years represented 13.90 percent. These findings suggested that most respondents had moderate to extensive experience in the microfinance sector, indicating familiarity with institutional operations and fraud detection practices. The presence of both less experienced and highly experienced employees reflected a balanced mix of perspectives. In conclusion, the experience profile demonstrated a knowledgeable workforce, which enhanced the reliability of responses regarding the effectiveness of flagging systems (Figure 4).

In relation to exposure to fraud detection activities, the results revealed that respondents with high exposure constituted 25.90 percent, representing the largest group. This was followed by those with moderate exposure at 19.40 percent, low exposure and no exposure each at 18.50 percent, and very high exposure at 17.60 percent. These findings indicated that the majority of respondents had at least moderate involvement in fraud detection activities. This suggested that most participants were sufficiently engaged in operational processes related to flagging systems. In conclusion, the exposure levels demonstrated that respondents were generally familiar with fraud detection activities, thereby supporting the validity of their responses (Figure 4).

Regarding ICT proficiency, the results indicated that respondents with very low proficiency constituted the highest proportion at 27.80 percent. This was followed by those with high and low proficiency at 20.40 percent each, very high proficiency at 17.60 percent, and moderate proficiency at 13.90 percent. These findings suggested that while some respondents possessed strong ICT skills, a significant proportion still had low digital proficiency. This variation could influence how effectively staff interacted with automated flagging systems. In conclusion, the mixed level of ICT proficiency highlighted potential disparities in system usage capability, which may affect fraud detection efficiency (Figure 4).

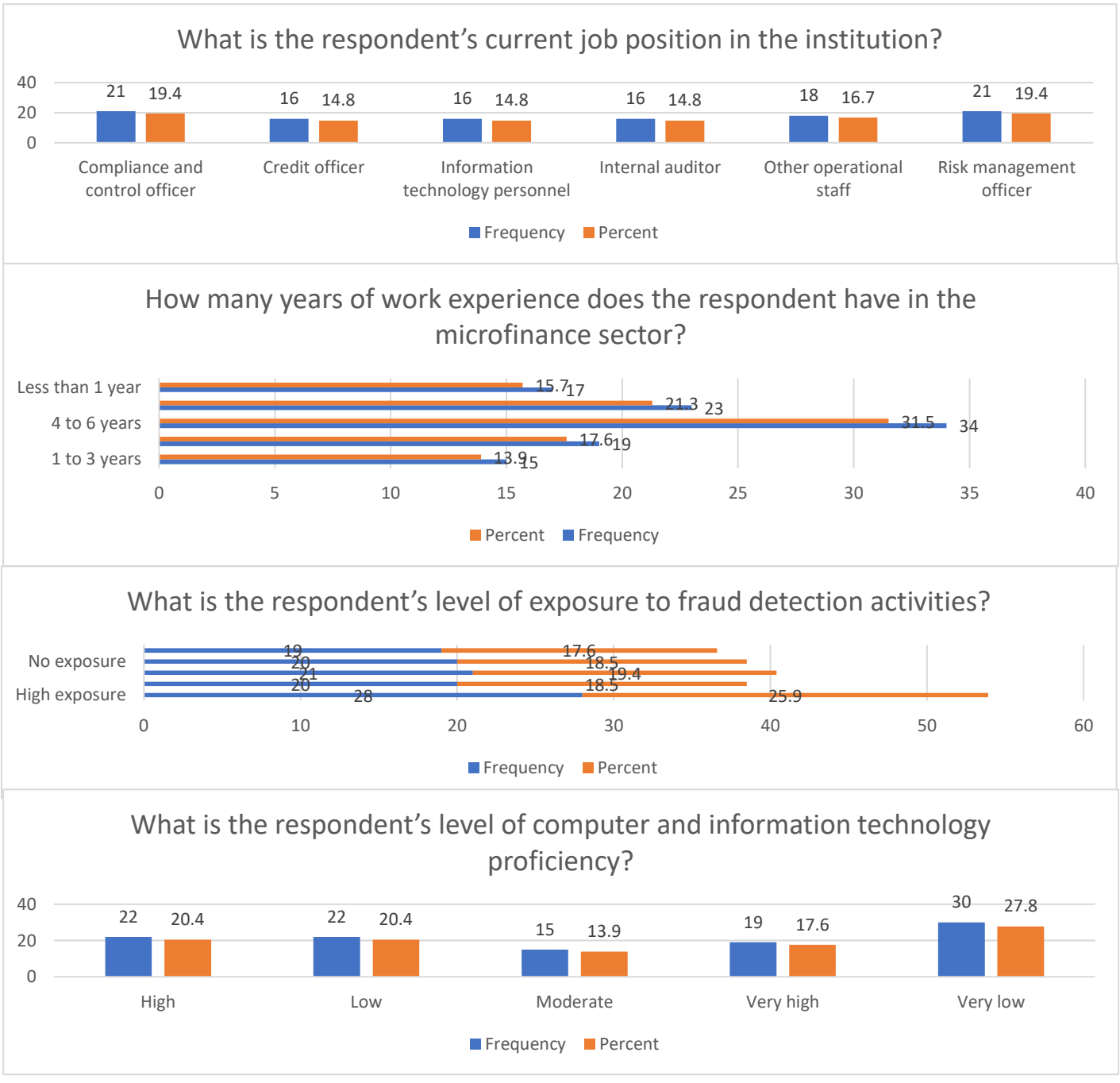

Figure 4. Respondents' job position, exposure to fraud detection and technology proficiency

Standard flagging systems that microfinance institutions use to detect fraud in Lusaka district of Zambia

The results indicated that integrated core banking system flagging modules were the most commonly used systems, accounting for 23.10 percent of respondents. This was closely followed by manual paper based monitoring and spreadsheet based monitoring systems, each representing 21.30 percent. Standalone electronic fraud detection software accounted for 19.40 percent, while advanced automated artificial intelligence based detection systems were the least utilised at 14.80 percent.

These findings suggest that fraud detection practices remained dependent on hybrid systems rather than fully advanced technologies. The continued use of manual and spreadsheet tools indicates weaker control activities and slower monitoring under the Committee of Sponsoring Organizations of the Treadway Commission framework. However, integrated core banking systems reflect progress toward stronger information systems and automated controls. In conclusion, fraud detection remained transitional, combining traditional and digital approaches that may affect efficiency and timely fraud identification (see Table 2).

The results revealed that a large proportion of respondents indicated that the institution relies on automated digital flagging systems to a large extent, accounting for 26.90 percent. This was followed by moderate extent at 22.20 percent and very large extent at 21.30 percent. Respondents who indicated no reliance at all constituted 13.90 percent, while those reporting reliance to a small extent accounted for 15.70 percent.

These findings suggest that although automated systems were increasingly used, reliance differed across institutions. Under the COSO framework, greater reliance supports stronger monitoring and risk assessment, while limited reliance implies continued dependence on weaker manual controls. The combined moderate to very large responses indicate movement toward digital fraud management, though uneven adoption may reduce sector wide effectiveness. In conclusion, automation was progressing but remained inconsistent across institutions (see Table 2).

The results indicated that the most common frequency of updating flagging system rules and detection parameters was once per year, accounting for 25.00 percent of respondents. This was followed by never updating at 21.30 percent and quarterly updates at 18.50 percent. Both once every two years and twice per year categories each accounted for 17.60 percent of respondents.

These findings suggest that update practices were inconsistent across institutions. Within the COSO framework, regular updates strengthen monitoring activities and ensure controls respond to changing fraud risks. Institutions that never update may face obsolete detection rules and weaker adaptability, while quarterly or annual updates reflect more proactive governance. In conclusion, infrequent updating may reduce the responsiveness and effectiveness of flagging systems against evolving fraud threats (see Figure 2).

Table 2. Distribution of Responses on Types, Reliance, and Updating Frequency of Institutional Flagging Systems for Fraud Detection

Which type of flagging system is primarily used by the institution to detect fraudulent activities?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Advanced automated artificial intelligence based detection systems	16	14.8	14.8	14.8
	Integrated core banking system flagging modules	25	23.1	23.1	38.0
	Manual paper-based monitoring	23	21.3	21.3	59.3
	Spreadsheet based monitoring systems	23	21.3	21.3	80.6
	Standalone electronic fraud detection software	21	19.4	19.4	100.0
	Total	108	100.0	100.0	

To what extent does the institution rely on automated digital flagging systems for fraud detection?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	15	13.9	13.9	13.9
	To a large extent	29	26.9	26.9	40.7
	To a moderate extent	24	22.2	22.2	63.0
	To a small extent	17	15.7	15.7	78.7
	To a very large extent	23	21.3	21.3	100.0
	Total	108	100.0	100.0	

How frequently does the institution update its flagging system rules and detection parameters?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Never	23	21.3	21.3	21.3
	Once every two years	19	17.6	17.6	38.9
	Once per year	27	25.0	25.0	63.9
	Quarterly	20	18.5	18.5	82.4
	Twice per year	19	17.6	17.6	100.0
	Total	108	100.0	100.0	

The effectiveness of current flagging systems used by Microfinance institutions in detecting fraud in Lusaka district of Zambia

The results indicated that highly effective and very highly effective responses each accounted for 20.40 percent of respondents. Moderately effective responses also represented 20.40 percent, while those who reported not effective constituted 21.30 percent. Slightly effective responses accounted for 17.60 percent. These findings suggested that perceptions regarding the effectiveness of flagging systems were mixed across respondents.

While many respondents viewed the systems as effective, a similar proportion questioned their performance. Under the Committee of Sponsoring Organizations of the Treadway Commission, this reflects uneven control activities and monitoring quality across institutions. Differences in technology, staff competence, and implementation may explain the varied perceptions. In conclusion, flagging systems were viewed as moderately effective overall, with no clear consensus on strong performance, suggesting inconsistent fraud detection outcomes.

The results further showed that real time detection was the most frequently reported response at 25.90 percent. This was followed by detection within 4 to 7 days at 24.10 percent and detection within 2 to 3 days at 20.40 percent. Detection taking more than 7 days accounted for 15.70 percent, while detection within 24 hours represented 13.90 percent. These findings suggested that although some institutions achieved prompt detection, many still faced delays. Within the COSO framework, faster detection indicates stronger information systems and monitoring processes, while delayed responses suggest weaker operational efficiency. The variation reflects differences in system sophistication and internal controls. In conclusion, detection speed was uneven, showing that real time fraud monitoring had not been consistently achieved across institutions (Table 3).

The results indicated that slight reduction was the most common response at 24.10 percent, followed by no reduction at 22.20 percent and very large reduction at 19.40 percent. Large reduction accounted for 18.50 percent, while moderate reduction represented 15.70 percent. These findings suggested that the impact of flagging systems on reducing fraud incidence was not uniformly strong across institutions. Some institutions experienced notable fraud reduction, while others reported little or no change. Under the COSO framework, this suggests differences in the effectiveness of monitoring, enforcement, and control activities. Where systems are well implemented, fraud reduction is stronger, but weak adoption limits results. In conclusion, flagging systems produced a modest overall impact, with outcomes varying considerably across institutions (Table 3).

Table 3. Distribution of Responses on the Effectiveness, Detection Speed, Fraud Reduction Impact, Alert Accuracy, and Specific Fraud Detection Performance of Institutional Flagging Systems

How effective are the current flagging systems in detecting fraudulent activities in general within the institution?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Highly effective	22	20.4	20.4	20.4
	Moderately effective	22	20.4	20.4	40.7
	Not effective	23	21.3	21.3	62.0
	Slightly effective	19	17.6	17.6	79.6
	Very highly effective	22	20.4	20.4	100.0
	Total	108	100.0	100.0	

How quickly do the flagging systems detect suspicious transactions after they occur?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2 to 3 days	22	20.4	20.4	20.4
	4 to 7 days	26	24.1	24.1	44.4
	In real time	28	25.9	25.9	70.4
	More than 7 days	17	15.7	15.7	86.1
	Within 24 hours	15	13.9	13.9	100.0
	Total	108	100.0	100.0	
To what extent have the flagging systems reduced the overall incidence of fraud in the institution?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Large reduction	20	18.5	18.5	18.5
	Moderate reduction	17	15.7	15.7	34.3
	No reduction	24	22.2	22.2	56.5
	Slight reduction	26	24.1	24.1	80.6
	Very large reduction	21	19.4	19.4	100.0
	Total	108	100.0	100.0	

How accurate are the alerts generated by the flagging systems in correctly identifying fraudulent cases?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Accurate	21	19.4	19.4	19.4
	Inaccurate	18	16.7	16.7	36.1
	Moderately accurate	31	28.7	28.7	64.8
	Very accurate	20	18.5	18.5	83.3
	Very inaccurate	18	16.7	16.7	100.0
	Total	108	100.0	100.0	
How effective are the flagging systems in detecting identity fraud, loan application fraud, multiple borrowing fraud, and intentional default?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Highly effective	25	23.1	23.1	23.1
	Moderately effective	24	22.2	22.2	45.4
	Not effective	17	15.7	15.7	61.1
	Slightly effective	21	19.4	19.4	80.6
	Very highly effective	21	19.4	19.4	100.0
	Total	108	100.0	100.0	

The results revealed that moderately accurate alerts were the most common response at 28.70 percent. Accurate alerts accounted for 19.40 percent, while very accurate alerts represented 18.50 percent. Both inaccurate and very inaccurate responses each accounted for 16.70 percent. These findings suggested that the accuracy of fraud detection alerts was generally perceived as moderate, with a balanced distribution between

accurate and inaccurate outcomes (Table 3). This indicated that while flagging systems were useful in identifying potential fraud, they also generated false positives or missed some cases, reducing reliability. Under the Committee of Sponsoring Organizations of the Treadway Commission, this reflects moderate monitoring effectiveness and weaknesses in information quality. In conclusion, alert accuracy was moderate, showing need for stronger precision, better data quality, and fewer detection errors.

The results showed that highly effective responses accounted for 23.10 percent, while moderately effective responses represented 22.20 percent. Very highly effective and slightly effective responses each accounted for 19.40 percent, whereas not effective responses constituted 15.70 percent. These findings suggested that flagging systems were generally perceived as moderately effective in detecting various forms of fraud, including identity fraud, loan application fraud, multiple borrowing fraud, and intentional default. However, responses showing limited effectiveness suggest that detection performance differed by fraud type and system design. Within the COSO framework, stronger control activities improve fraud identification, while weak configuration reduces consistency. In conclusion, flagging systems showed moderate effectiveness in detecting different fraud forms, though uneven performance remained across institutions (Table 3).

Challenges faced by microfinance institutions in using flagging systems to detect fraud in Lusaka district of Zambia

The results indicated that responses were relatively distributed across all categories, with both “not at all” and “to a small extent” each accounting for 20.40 percent. “To a moderate extent” accounted for 21.30 percent, while “to a very large extent” represented 19.40 percent. “To a large extent” accounted for 18.50 percent. These findings suggest that technical system limitations were perceived in a mixed manner, with no dominant response category.

While some respondents reported limited hindrance, others indicated moderate to high constraints. Under the Committee of Sponsoring Organizations of the Treadway Commission, this reflects uneven control infrastructure and monitoring capacity across institutions. In conclusion, technical limitations had a moderate and inconsistent effect on fraud detection effectiveness (Table 4).

The results showed that “not at all” was the most common response at 25.00 percent, followed by “to a moderate extent” at 24.10 percent and “to a very large extent” at 22.20 percent. “To a small extent” accounted for 15.70 percent, while “to a large extent” represented 13.00 percent. These findings suggest that perceptions of insufficient staff training as a challenge were varied.

While many respondents did not view training as a major issue, others reported serious concerns. Within the COSO framework, staff competence supports effective control activities and monitoring. Weak training may reduce proper use of systems and response to alerts. In conclusion, insufficient training remained a mixed but notable challenge to flagging system effectiveness (Table 4). The results indicated that “to a large extent” was the most frequently reported response at 25.90 percent, followed by “to a very large extent” at 21.30 percent. “Not at all” accounted for 19.40 percent, while both “to a moderate extent” and “to a small extent” each represented 16.70 percent. These findings suggest that poor quality or incomplete customer data was generally perceived as a significant factor affecting flagging system performance.

A strong combined response at higher levels indicates that data quality was a major operational concern. Under the COSO framework, weak information quality undermines reliable monitoring and decision making. In conclusion, customer data quality significantly influenced flagging system effectiveness, although impacts varied across institutions (Table 4). The results revealed that “to a moderate extent” was the most common response at 25.90 percent, followed by “to a large extent” at 24.10 percent. “Not at all” and “to a very large extent” each accounted for 17.60 percent, while “to a small extent” represented 14.80 percent. These findings suggest that false alerts were considered a moderately serious operational challenge. High and low responses indicate inconsistent system precision. Within the COSO framework, frequent false positives weaken monitoring efficiency, increase workload, and reduce trust in controls. In conclusion, false alerts presented a moderate operational challenge with varying severity across institutions (Table 4).

Table 4. Distribution of Responses on Technical, Training, Data Quality, False Alert, and Regulatory Challenges Affecting the Effectiveness of Flagging Systems for Fraud Detection

To what extent do technical system limitations hinder effective use of flagging systems for fraud detection?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	22	20.4	20.4	20.4
	To a large extent	20	18.5	18.5	38.9
	To a moderate extent	23	21.3	21.3	60.2
	To a small extent	22	20.4	20.4	80.6
	To a very large extent	21	19.4	19.4	100.0
	Total	108	100.0	100.0	

How significant is the challenge of insufficient staff training in the effective use of flagging systems?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	27	25.0	25.0	25.0
	To a large extent	14	13.0	13.0	38.0
	To a moderate extent	26	24.1	24.1	62.0
	To a small extent	17	15.7	15.7	77.8
	To a very large extent	24	22.2	22.2	100.0
	Total	108	100.0	100.0	

To what extent does poor quality or incomplete customer data affect the performance of flagging systems?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	21	19.4	19.4	19.4
	To a large extent	28	25.9	25.9	45.4
	To a moderate extent	18	16.7	16.7	62.0
	To a small extent	18	16.7	16.7	78.7
	To a very large extent	23	21.3	21.3	100.0
	Total	108	100.0	100.0	

How serious is the problem of false alerts, including excessive false positives, in daily operations?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	19	17.6	17.6	17.6
	To a large extent	26	24.1	24.1	41.7
	To a moderate extent	28	25.9	25.9	67.6
	To a small extent	16	14.8	14.8	82.4
	To a very large extent	19	17.6	17.6	100.0
	Total	108	100.0	100.0	

To what extent do institutional policy and regulatory constraints limit the effective use of flagging systems?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	25	23.1	23.1	23.1
	To a large extent	22	20.4	20.4	43.5
	To a moderate extent	24	22.2	22.2	65.7
	To a small extent	18	16.7	16.7	82.4
	To a very large extent	19	17.6	17.6	100.0
	Total	108	100.0	100.0	

The results showed that “not at all” accounted for 23.10 percent, followed by “to a moderate extent” at 22.20 percent and “to a large extent” at 20.40 percent. “To a small extent” represented 16.70 percent, while “to a

very large extent" accounted for 17.60 percent. These findings suggest that policy and regulatory constraints were perceived in a mixed manner. While many respondents indicated limited impact, others reported moderate to high constraints. Under the Committee of Sponsoring Organizations of the Treadway Commission, policies shape control activities, compliance, and monitoring processes. Rigid or unclear regulations may weaken system responsiveness, while supportive frameworks enhance controls. In conclusion, policy and regulatory constraints moderately influenced flagging system effectiveness, with impacts differing across institutions (Table 4).

Inferential statistics: Regression analysis

The regression results presented in Table 4 indicated that the selected explanatory variables had a moderate relationship with the effectiveness of fraud detection among registered microfinance institutions in Lusaka. The model summary showed a correlation coefficient of R = 0.487, which suggested that the combined predictors were positively associated with variations in fraud detection effectiveness. This implied that changes in staff training exposure, system interaction frequency, reliance on automated flagging systems, technical limitations, staff training challenges, and policy constraints were related to changes in the dependent variable. Although the relationship was not extremely strong, it was sufficiently meaningful to indicate that institutional and operational factors played an important role in determining how effectively fraud was detected within the institutions examined.

The coefficient of determination showed an R Square value of 0.237, meaning that 23.70 percent of the variation in fraud detection effectiveness was explained by the variables included in the model. This suggested that nearly one quarter of the observed differences in effectiveness were attributable to the identified predictors. The remaining 76.30 percent was explained by other factors not captured in the model, such as management commitment, organisational culture, fraud complexity, quality of internal controls, employee ethics, technological sophistication, or external economic pressures. The adjusted R Square value of 0.192 further indicated that after accounting for the number of predictors used, the model still explained 19.20 percent of the variation. This confirmed that the model had practical explanatory value, although fraud detection effectiveness was influenced by a broader range of factors beyond those measured (see Table 5).

The ANOVA results reported an F statistic of 5.232 with a significance level of 0.000. This indicated that the regression model as a whole was statistically significant and that the predictors jointly provided a better explanation of fraud detection effectiveness than a model with no independent variables. In practical terms, the evidence suggested that the combined institutional and operational factors were relevant in explaining why some microfinance institutions performed better than others in detecting fraud. The significance of the model demonstrated that the selected variables should not be viewed in isolation, since their collective influence materially shaped fraud detection outcomes.

The constant term was reported as 1.553 and was statistically significant at 0.000. This implied that even when all explanatory variables were held constant, a baseline level of fraud detection effectiveness still existed. Such a baseline may reflect minimum internal procedures, routine supervision, or standard regulatory compliance measures already embedded within institutions regardless of the specific predictors considered in the model (see Table 5).

Formal training related to fraud detection and monitoring produced a positive coefficient of 0.085 and was statistically significant at 0.048. This result suggested that an increase in the number of trainings attended was associated with improved fraud detection effectiveness. It was therefore indicated that capacity building strengthened employee competence in recognising suspicious patterns, interpreting alerts, and responding appropriately to flagged transactions. This finding aligned with the COSO framework, particularly the control environment and monitoring dimensions, since well trained staff are more likely to uphold internal controls and apply systems effectively. The result further implied that institutions investing in continuous professional development were likely to achieve stronger fraud prevention outcomes than those neglecting staff learning. The frequency with which respondents interacted with the institutional flagging system had a positive coefficient of 0.064, but the significance level of 0.125 indicated that the effect was not statistically significant. This meant that although more frequent interaction appeared associated with better fraud detection, the

evidence was insufficient to conclude that interaction alone materially improved outcomes. The result may indicate that merely accessing or using the system regularly was not enough unless such interaction was supported by quality training, management follow up, and technically efficient systems. It also suggested that repeated exposure without adequate competence or authority to act on alerts may not generate measurable gains in fraud detection effectiveness (see Table 5).

Table 5. The effectiveness of flagging systems in detecting fraud among registered micro-finance institutions in Lusaka

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.487[a]	.237	.192	.60831
a. Predictors: (Constant), To what extent do institutional policy and regulatory constraints limit the effective use of flagging systems?, To what extent do technical system limitations hinder effective use of flagging systems for fraud detection?, How significant is the challenge of insufficient staff training in the effective use of flagging systems?, To what extent does the institution rely on automated digital flagging systems for fraud detection?, How frequently does the respondent interact with the institutional flagging system?, How many formal trainings related to fraud detection and monitoring has the respondent attended?				

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.617	6	1.936	5.232	.000[b]
	Residual	37.374	101	.370		
	Total	48.991	107			
a. Dependent Variable: Effectiveness of fraud detection among microfinance institutions in Lusaka Zambia (Dependent Variable)						
b. Predictors: (Constant), To what extent do institutional policy and regulatory constraints limit the effective use of flagging systems?, To what extent do technical system limitations hinder effective use of flagging systems for fraud detection?, How significant is the challenge of insufficient staff training in the effective use of flagging systems?, To what extent does the institution rely on automated digital flagging systems for fraud detection?, How frequently does the respondent interact with the institutional flagging system?, How many formal trainings related to fraud detection and monitoring has the respondent attended?						

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.553	.340		4.571	.000
	How many formal trainings related to fraud detection and monitoring has the respondent attended?	.085	.043	.178	2.005	.048
	How frequently does the respondent interact with the institutional flagging system?	.064	.041	.136	1.546	.125
	To what extent does the institution rely on automated digital flagging systems for fraud detection?	.126	.043	.259	2.953	.004
	To what extent do technical system limitations hinder effective use of flagging systems for fraud detection?	-.131	.045	-.256	-2.934	.004
	How significant is the challenge of insufficient staff training in the effective use of flagging systems?	-.064	.043	-.133	-1.503	.136
	To what extent do institutional policy and regulatory constraints limit the effective use of flagging systems?	-.079	.042	-.165	-1.875	.064
a. Dependent Variable: Effectiveness of fraud detection among microfinance institutions in Lusaka Zambia (Dependent Variable)						

Reliance on automated digital flagging systems produced a positive coefficient of 0.126 and was statistically significant at 0.004. This indicated that greater dependence on automated systems significantly improved fraud detection effectiveness. Institutions making stronger use of digital tools were likely to benefit from faster transaction monitoring, quicker identification of anomalies, and reduced human error. The standardised beta coefficient of 0.259 showed that this variable was among the strongest positive predictors in the model. This finding reinforced the importance of digital transformation in financial risk management and suggested that technology adoption had become central to effective fraud detection in the microfinance sector. Within the COSO framework, this reflected stronger information and communication systems together with enhanced monitoring activities (see Table 5).

Technical system limitations recorded a negative coefficient of -0.131 and were statistically significant at 0.004. This indicated that as technical constraints increased, fraud detection effectiveness significantly declined. Problems such as system downtime, poor integration, slow processing, outdated software, and unreliable infrastructure were therefore shown to weaken institutional capacity to detect fraud. The standardised beta of -0.256 suggested that technical limitations were one of the strongest predictors in the model, but in a harmful direction. This meant that even where institutions intended to strengthen fraud monitoring, poor technology infrastructure could substantially reduce performance. The finding highlighted the practical necessity of system upgrades, maintenance, and adequate technological investment (see Table 5).

Insufficient staff training as an operational challenge had a negative coefficient of -0.064, but the significance level of 0.136 showed that the effect was not statistically significant. Although the direction suggested that training gaps may reduce effectiveness, the evidence did not support a strong independent effect when other variables were considered simultaneously. This may imply that the number of trainings attended captured training influence more effectively than subjective perceptions of insufficiency. It may also indicate that some institutions compensated for limited formal training through supervision, experience, or peer support.

Institutional policy and regulatory constraints produced a negative coefficient of -0.079 with a significance level of 0.064. This result suggested that more restrictive policies or regulatory barriers tended to reduce fraud detection effectiveness, although the effect was not statistically significant at the conventional 5 percent level. The finding implied that cumbersome approval processes, rigid compliance requirements, or unclear regulatory expectations may slow responses to suspicious transactions. However, because significance was marginal, the evidence suggested that policy constraints were less decisive than technology and automation factors in shaping fraud detection outcomes (see Table 5).

Overall, the regression results showed that fraud detection effectiveness among registered microfinance institutions in Lusaka was shaped most strongly by practical organisational capabilities rather than routine procedural presence alone. Positive outcomes were linked to staff development and stronger reliance on automated systems, while negative outcomes were associated with technical weaknesses. Variables such as system interaction frequency, perceived training shortages, and regulatory constraints showed weaker independent influence once other factors were controlled for.

In conclusion, this study established that effective fraud detection depended on a combination of competent personnel, reliable technology, and meaningful automation. The most influential drivers of improved effectiveness were formal fraud related training and institutional reliance on automated digital flagging systems, while technical system limitations significantly undermined performance. The findings therefore suggested that microfinance institutions seeking stronger fraud control should prioritise technological modernisation, regular employee training, and system reliability in order to enhance institutional resilience and reduce fraud exposure.

Results from qualitative analysis

Flagging Systems and Fraud Response Procedures

Respondents explained that institutions used a combination of automated and manual flagging systems to detect identity fraud, loan application fraud, multiple borrowing, and intentional default. The findings showed

that fraud detection was based on a hybrid environment where technology and human review operated together. Many participants indicated that integrated core banking systems formed the primary detection mechanism because they automatically generated alerts when unusual patterns appeared. One respondent stated that *"the core banking system flags accounts when there are repeated loan applications within a short period or when identity details do not match existing records"*. This demonstrated that automated controls were embedded within routine institutional operations.

Participants also described the continued use of spreadsheet based monitoring tools, especially for tracking repayment patterns and identifying multiple borrowing cases across branches. One respondent explained that *"we maintain Excel sheets that compare borrower details across branches to detect customers who try to borrow more than once under different names"*. This suggested that manual data consolidation remained important where fully integrated systems were limited.

Some respondents further noted that manual paper based verification was still used, particularly during loan application screening. Physical files and supporting documents were reviewed before approval decisions were finalized. This process was considered important in preventing identity fraud at the earliest stage.

A smaller number of participants referred to advanced technologies such as artificial intelligence based systems and standalone fraud detection software. These tools were described as useful for anomaly detection and real time monitoring. One respondent stated that *"alerts are generated instantly when suspicious logins or transaction patterns are detected"*. However, many indicated that such technologies were still at early stages of adoption.

When suspicious activity was flagged, respondents reported that institutions followed a structured response process involving verification by compliance or risk officers, review of customer records, and collaboration among departments such as IT, audit, credit, and management. Confirmed fraud often resulted in account freezes, transaction suspension, escalation, or recovery action. Overall, the findings showed that institutions relied on multiple complementary systems, but effectiveness varied according to technological maturity, staff capacity, and coordination mechanisms.

Effectiveness, Accuracy, Response Time, and Fraud Prevention Outcomes

Respondents described the effectiveness of current flagging systems as moderate to high, depending on the type of fraud being detected. Identity fraud was widely viewed as the area where systems performed best because automated checks could compare names, identification numbers, and customer records. One participant noted that *"the system is very effective in detecting duplicate identities and repeated loan applications because it automatically cross checks customer data across the entire database"*. This indicated that centralized data systems strengthened early fraud detection.

For loan application fraud and multiple borrowing, respondents reported more mixed experiences. Systems were able to identify duplicate borrowing within the same institution, but were less effective when customers used different branches or altered personal details. This suggested that fraud detection performance depended heavily on branch integration and data quality.

Intentional default was considered more difficult to detect because it often involved behavioural patterns rather than immediate transactional irregularities. Some respondents explained that delayed instalments or unusual repayment trends triggered warnings, but in many cases fraud was only recognized after losses had already occurred. This reflected weaker predictive capability in relation to repayment behaviour.

Participants further indicated that automation had improved fraud detection accuracy by reducing human error and increasing consistency. However, false positives remained a common challenge. Staff often had to manually review alerts before action could be taken. In terms of response time, real time alerts were considered a major improvement because suspicious transactions could be identified before completion. One respondent stated that *"alerts are now generated instantly, which allows staff to respond before the transaction is fully completed"*.

Despite these gains, some respondents noted that excessive alerts created delays because staff were overwhelmed by the number of cases requiring review. Prevention outcomes were therefore mixed. Some institutions reported reduced fraud incidence due to early detection, while others argued that fraudsters had adapted their methods to bypass controls. Overall, the findings suggested that flagging systems had strengthened fraud management, but their effectiveness remained constrained by false alerts, system gaps, and evolving fraud techniques.

Challenges Affecting Flagging Systems and Proposed Improvement Measures

Respondents identified several technical, operational, and institutional challenges that reduced the effectiveness of flagging systems. A major technical issue was weak system integration across branches and platforms. Many participants explained that fraud committed in one branch was not always immediately visible elsewhere. One respondent stated that *"the main challenge is that some systems are not fully integrated, so fraud that happens in one branch is not always visible in another branch immediately"*. This weakened the detection of multiple borrowing and cross branch fraud.

Outdated technology was also frequently mentioned. Some institutions were still using older systems that lacked advanced automation or real time monitoring capabilities. As a result, fraud detection processes were slower and less accurate. Operational challenges included alert overload, where systems generated too many warnings for staff to investigate efficiently. One participant explained that *"the system produces too many alerts at once, and staff struggle to investigate all of them properly"*. This created delays and increased the possibility of serious fraud cases being overlooked.

Insufficient staff training was another recurring concern. Respondents noted that some employees lacked the skills needed to interpret alerts or use digital tools effectively. Human limitations therefore reduced the benefits of otherwise functional systems. Institutional challenges were also highlighted, particularly poor communication between departments and inconsistent procedures for handling flagged cases. Weak coordination between IT, credit, audit, and risk teams often slowed down decision making.

Data quality problems were considered especially serious. Incomplete or inaccurate customer information sometimes caused systems to miss genuine fraud or wrongly flag legitimate transactions. This reduced trust in automated alerts and increased the need for manual verification.

To improve performance, respondents recommended full system integration across branches, continuous staff training, refinement of rules to reduce false alerts, and stronger institutional coordination. Clear procedures for handling flagged cases were also considered necessary. Overall, the findings showed that while flagging systems had improved fraud detection, their full potential could only be achieved through technological upgrades, better data management, skilled personnel, and stronger organizational alignment.

DISCUSSION

The finding that technical system limitations had a moderate and inconsistent impact aligns with Nyirenda (2024), who identified technological limitations as a key factor affecting microfinance institution performance in Lusaka. Nyirenda reported that many institutions operated with outdated hardware and software, limiting their ability to implement advanced digital fraud detection features. In this study, respondents similarly reported mixed perceptions regarding technical constraints. The regression results further confirmed a statistically significant negative effect of technical system limitations on fraud detection effectiveness ($B = -0.131$, $p = 0.004$). This indicated that increased technical weaknesses reduced the ability of flagging systems to detect fraud effectively. Musyoki (2023) similarly argued that weak technological infrastructure creates gaps in monitoring and weakens internal control efficiency. The results therefore suggest that technology quality is not only a perceived challenge but a measurable determinant of fraud detection performance.

The finding on staff training gaps is consistent with Ramadhany (2025), who found that self efficacy and fraud awareness significantly improve fraud detection effectiveness. Ramadhany showed that auditors with stronger professional knowledge were more effective in identifying fraud indicators. In this study, perceptions of

insufficient training were mixed, indicating uneven capacity development. However, regression results showed that actual training attendance had a significant positive effect on fraud detection effectiveness (B = 0.085, p = 0.048), while perceived training insufficiency was not statistically significant (B = -0.064, p = 0.136). This suggests that practical exposure through formal training is more influential than general perceptions of training gaps. Boateng, Boateng, and Acquah (2020) similarly emphasised that inadequate training increases fraud vulnerability in microfinance institutions. The findings therefore highlight the importance of continuous structured training in strengthening detection capability.

The finding that poor quality or incomplete customer data significantly affects system performance supports Agubata (2022), who noted that effective fraud detection depends on accurate and complete data inputs. In this study, respondents indicated that data quality issues had a strong impact on system performance. Although not directly tested as a regression variable, its importance is reflected in the significant positive effect of reliance on automated systems (B = 0.126, p = 0.004), which depend heavily on data accuracy. Mubita (2023) similarly found that poor data quality weakens fraud detection in financial systems in Lusaka. This suggests that automation alone is insufficient without reliable underlying data structures.

The finding on false alerts aligns with Yucel (2020), who observed that red flag systems often generate false positives that require additional verification, reducing efficiency. In this study, false alerts were viewed as a moderate challenge with varying intensity across institutions. This reflects inconsistency in system calibration and monitoring quality. Musyoki (2023) further noted that repeated false alerts may reduce staff responsiveness to genuine warnings. The regression findings also showed that while automation improved fraud detection effectiveness, system configuration quality determines whether benefits outweigh false alert costs. This indicates that effectiveness depends not only on system use but also on system accuracy and maintenance.

The finding that policy and regulatory constraints had a moderate influence is consistent with Taranhike and Bwalya (2025), who reported that regulatory requirements can limit operational flexibility in microfinance institutions in Lusaka. This study found mixed perceptions regarding regulatory constraints. Regression results showed a negative but marginally insignificant effect (B = -0.079, p = 0.064), suggesting that policy constraints may reduce effectiveness but are less influential than technological and automation factors. Yolanda (2013) similarly noted that weak institutional frameworks can hinder fraud control implementation. The findings therefore suggest that regulatory environments influence fraud detection indirectly through operational efficiency.

The regression model results further strengthen the discussion by showing a statistically significant overall model fit (F = 5.232, p = 0.000). The model explained 23.70 percent of the variation in fraud detection effectiveness, indicating that institutional and operational factors jointly influence outcomes. This confirms that fraud detection is not determined by a single factor but by a combination of technology, training, automation, and institutional conditions.

Hence, the discussion indicates that fraud detection effectiveness depends on the integration of reliable technology, adequate staff training, strong data systems, and supportive institutional environments. Technical weaknesses and poor system quality reduce effectiveness, while automation and training improve it. These findings align with the Committee of Sponsoring Organizations of the Treadway Commission, which emphasises control activities, monitoring, and information quality as core drivers of effective internal control systems.

CONCLUSION

The study concluded that microfinance institutions in Lusaka used a combination of fraud detection systems, with integrated core banking flagging modules being the most common. Manual paper based monitoring and spreadsheet systems were also widely used, while standalone electronic tools were less common and artificial intelligence based systems were minimally adopted. This indicated that fraud detection environments remained hybrid and transitional, combining traditional and modern methods. Uneven adoption of advanced systems and irregular updating practices limited institutional readiness against emerging fraud risks.

The regression results further confirmed that these system differences had a measurable influence on fraud detection effectiveness. The model was statistically significant (F = 5.232, p = 0.000) and explained 23.70 percent of the variation in effectiveness, indicating that institutional and operational factors collectively shaped fraud detection outcomes. Reliance on automated digital flagging systems significantly improved effectiveness (B = 0.126, p = 0.004), while technical system limitations significantly reduced effectiveness (B = -0.131, p = 0.004). This demonstrated that technology quality and automation were key determinants of performance within the institutions studied.

The study further concluded that the effectiveness of current flagging systems was moderate overall. Some institutions reported high effectiveness, real time detection, and improved fraud prevention outcomes, while others experienced delayed detection, inaccurate alerts, and limited fraud reduction. These differences were explained by variations in system automation, staff training exposure, and technological capacity. Formal training attendance had a positive and significant effect on fraud detection effectiveness (B = 0.085, p = 0.048), confirming that human capacity development improved system performance. However, interaction frequency with systems, perceived training insufficiency, and policy constraints did not show strong statistically significant effects, indicating that effectiveness depended more on structural and technological factors than routine usage alone.

The study also concluded that several challenges constrained the use of flagging systems. These included weak technological infrastructure, poor data quality, inadequate staff training, false alerts, and policy or regulatory limitations. Although some of these challenges were not all statistically significant in isolation, the overall regression model confirmed that they jointly influenced system effectiveness. False alerts, in particular, reflected inconsistencies in system configuration, while data quality and technical limitations had broader implications for system reliability and accuracy.

Based on these findings, it was concluded that improving fraud detection in microfinance institutions requires strengthening system integration through centralized digital platforms that support real time monitoring. Gradual adoption of advanced technologies such as artificial intelligence based tools was considered necessary to enhance predictive capability. Regular system updates, ideally conducted quarterly, were important for maintaining relevance against evolving fraud patterns. Continuous staff training was essential for improving system interpretation and response accuracy, while stronger data quality controls through validation and auditing were necessary for reliable outputs. Refinement of detection models was also required to reduce false alerts and improve prioritisation of high risk transactions. Finally, regulatory bodies were expected to support minimum fraud detection standards, enhance compliance oversight, and encourage coordinated information sharing across institutions.

REFERENCES

1. Agubata, S. (2022). Alterness to red flags and fraud detection in micro finance banks in Awka Metropolis. From researchgate.net: https://www.researchgate.net/publication/ 358046345 ALERTNESS TO_RED_FLAGS_AND_FRAUD_DETECTION_IN_MICRO_FINANCE_BANKS_IN_AWKA_METROPOLIS
2. Arhinful, R., & Mensah, L. (2025). The Impact of Non-Performing Loans on Bank Growth: The Moderating Roles of Bank Size and Capital Adequacy Ratio—Evidence from U.S. Banks. From www.mdpi.com: https://www.mdpi.com/2227-7072/13/3/165
3. Arnold, R. D., & Wade, J. (2015). A Definition of Systems Thinking: A Systems Approach. From researchgate.net: https://www.researchgate.net/publication/273894661 A_Definition_of Systems_Thinking_A_Systems_Approach
4. Boateng, A. A., Boateng, G. O., & Acquah, H. E. (2020). A Literature Review of Fraud Risk Management in Micro Finance Institutions in Ghana. From researchgate.net: 345435639 A_Literature_Review_of_Fraud_Risk_Management_in_Micro_Finance_Institutions_in_Ghana
5. Chibawe, L., & Haabazoka, L. (2025). A Study of the Factors Influencing Bank Loan Performance in Zambian Commercial Banks. From researchgate.net: https://www.researchgate.net/publication/ 390905688_A_Study_of_the_Factors_Influencing_Bank_Loan_Performance_in_Zambian_Commercial_Banks

6. Chowdhury, M. (2025). Analyzing COSO Framework, Objectives, and Implementation. From academia.edu: https://www.academia.edu/128142695/Analyzing COSO_Framework Objectives_and_Implementation
7. Dolo, A. (2025). The role of microfinance in small, medium, and micro enterprises in Gqeberha. From files01.core.ac.uk: https://files01.core.ac.uk/download/660977880.pdf
8. Durgham, M. (2017). The use of Red Flag Indicators for improving the effectiveness of External Audit in detecting financial fraud. From researchgate.net: https://www.researchgate.net/publication/348976105_The_use_of_Red_Flag_Indicators_for_improving_the_effectiveness_of_External_Audit_in_detecting_financial_fraud
9. Funyina, T. K., & Muhanga, I. (2021). The Determinants of Non-Performing Loans in Zambia: Impact of Bank-Specific and Macroeconomic Variables. From boz.zm: https://www.boz.zm/TheDeterminantsofNonPerformingLoansinZambia.pdf
10. Hilal, W., Gadsden, A., & , . (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. From sciencedirect.com: https://www.sciencedirect.com/science/article/pii/S0957417421017164
11. Kalunga, B. (2017). The effects of financial inclusion on fostering economic growth and wealth creation in Zambia. From dspace.unza.zm: https://dspace.unza.zm/server/api/core/bitstreams/91ef20dc-ca60-40eb-a52b-d8dc3d327349/content
12. Kunc, M. (2024). The Systems Thinking Approach to Strategic Management. From www.mdpi.com: https://www.mdpi.com/2079-8954/12/6/213
13. Lyons, S. (2012). Internal Controls Integrated Framework: Response to COSO Public Draft Exposure. From researchgate.net: https://www.researchgate.net/publication/255728421 Internal_Controls_Integrated_Framework_Response_to_COSO_Public_Draft_Exposure
14. Mahlangu, L., & Chowa, T. (2022). An Investigation of The Causes and Challenges of Non-Performing Loans: A case of a Zambian Bank. From researchgate.net: https://www.researchgate.net/publication/361155722_An_Investigation_of_The_Causes_and_Challenges_of_Non-Performing_Loans_A_case_of_a_Zambian_Bank
15. Mubita, N. G. (2023). An investigation of the adequacy of control measures in combatting mobile money fraud in Lusaka district. From dspace.unza.zm: https://dspace.unza.zm/server/api/core/bitstreams/66925301-faae-47c8-809e-ea893772dc68/content
16. Musyoki, K. M. (2023). Internal Control Systems and their role in Financial Fraud Prevention in Kenya. From ijcsacademia.com: https://ijcsacademia.com/index.php/journal/article/view/174
17. Nyirenda, N. D. (2024). An assessment of critical success factors of microfinance institutions in Lusaka, Zambia. From dspace.unza.zm: https://dspace.unza.zm/server/api/core/bitstreams/118c7a29-c298-4094-9fc7-a681ad0df77f/content
18. Olufemi, B., Bello, O., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. From www.researchgate.net: https://www.researchgate.net/publication/383264952_Artificial_intelligence_in_fraud_prevention_Exploring_techniques_and_applications_challenges_and_opportunities
19. Paliyani, A., & Silwimba, P. (2025). Effectiveness of Microfinance Institutions in Enhancing Financial Access for SMEs: A Case Study of Lusaka, Zambia. From researchgate.net: https://www.researchgate.net/publication/399100378_Effectiveness_of_Microfinance_Institutions_in_Enhancing_Financial_Access_for_SMEs_A_Case_Study_of_Lusaka_Zambia
20. Pebruary, S., & Edward, M. Y. (2019). Fraud analysis in micro finance institution. From researchgate.net: https://www.researchgate.net/publication/331567613_Fraud_analysis_in_micro_finance_institution
21. Ramadhany, A. A. (2025). Enhancing Fraud Detection Performance: The Interplay of Red Flag Awareness, Self-Efficacy, and Professional Skepticism. From mdpi.com: https://www.mdpi.com/1911-8074/18/6/301
22. Renes, R. (2000). The Real Coso, and Nothing but the Real Coso. From researchgate.net: https://www.researchgate.net/publication/256046366_The_Real_Coso_and_Nothing_but_the_Real_Coso

23. Sichuundu, J. (2024). A Contextual Analysis of the Growth of Financial Inclusion in Zambia. From rsisinternational.org: https://rsisinternational.org/journals/ijriss/articles/a-contextual-analysis-of-the-growth-of-financial-inclusion-in-zambia
24. Sutton, R. T., Pincock, D., & Baumgart, D. C. (2020). An overview of clinical decision support systems: benefits, risks, and strategies for success. From pmc.ncbi.nlm.nih.gov: https://pmc.ncbi.nlm.nih.gov/articles/PMC7005290
25. Taranhike, K., & Bwalya, C. C. (2025). Examining the Effectiveness of Microfinance Institutions in Enhancing Economic Empowerment: A Case Study of Small and Medium Enterprises (SMEs) in the Food Processing Industry in Lusaka District. From research.icu.ac.zm: https://research.icu.ac.zm/storage/1293/archive-1750331890.pdf
26. Teresa , M. (2024). Internal Control in Companies from the Perspective of the COSO. From researchgate.net: https://www.researchgate.net/publication/382188030 Internal_Control_in Companies_from_the_Perspective_of_the_COSO
27. Tonui, A. K., Kamau, D., & Ombui, K. (2018). Effect of Forensic accounting services on Fraud detection on microfinance institutions in Bomet County. From researchpublish.com: https://www.researchpublish.com/upload/book/EFFECT%20OF%20FORENSIC%20ACCOUNTING-5767.pdf
28. Yolanda, A. A. (2013). Impact of Internal Control on Fraud Detection and Prevention in Microfinance Institutions. From diva-portal.org: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1578691&dswid=7924
29. Yucel, E. (2020). Effectiveness Of Red Flags in Detecting Fraudulent Financial Reporting: An Application In Turkey. From dergipark.org.tr: https://dergipark.org.tr/tr/download/article-file/427482
30. Zimba, A. (2025). Unveiling deception: a socio-economic analysis of smishing attacks on mobile money transaction users. From nature.com: https://www.nature.com/articles/s41599-025-06141-8.pdf