ISSN: 2958-2326

AJoCsOpen
Sharing Knowledge in Business

African Journal of Commercial Studies

Publisher's Home Page: https://ijcsacademia.com/

AFRICAN JOURNAL OF COMMERCIAL STUDIES

Research Paper | Peer Reviewed | Open Access

The Role of Financial Technologies in Enhancing Internal Control Effectiveness: Evidence from Indo Zambia Bank

Mwenya Mulenga[1]*

[1]*Graduate School of Business, University of Zambia*
* Corresponding Author

African Journal of Commercial Studies, 2026, 7(2),506–515
DOI Link: https://doi.org/10.59413/ajocs/v7.i2.42

Article Info

Volume 7, Issue 2

Publication history:
Accepted on 15 February 2026;
Published: 20 April 2026

Article DOI:
10.59413/ajocs/v7.i2.42

Abstract

This study explored the role of Financial Technologies (FinTech) in enhancing internal control effectiveness at Indo Zambia Bank, Lusaka, Zambia. The study utilized a convergent parallel mixed method design where 140 staff surveys were used, as well as qualitative interviews of ten key informants who were selected based on the compliance, internal audit, risk management, and digital operations departments. Three FinTech constructs were also studied automated monitoring systems, artificial intelligence-based fraud detection tools, and digital transaction platforms, and each of them was evaluated in terms of correlation with internal control effectiveness in terms of procedural efficiency, reporting reliability, and regulatory compliance. Results showed that there were weak yet statistically significant positive relations between FinTech adoption and internal control effectiveness (r=0.195 to r=0.291), which point to the fact that technology in itself is not enough to help control systems to their full extent. There was generally a positive perception of staff about procedural efficiency and automated reporting, though there were still gaps in proactive fraud prevention and cybersecurity preparedness, and back-office integration. The conclusion of the study is that the role of FinTech in the effectiveness of internal control is conditional depending on the governance structures, staff competency, vendor management and regulatory alignment. The paper suggests that the Indo Zambia Bank should focus on integrating back-office FinTech, enhancing proactive fraud detection, enforcing systematic governance and cybersecurity education, and enhancing oversight of the vendors. The results provide empirical research on the literature of digital banking governance in the developing economies and present feasible advice to management and policymakers.
Keywords: FinTech, internal control, digital banking, fraud detection, Zambia, banking governance

Keywords: Fintech, Internal Control, Digital Banking, Fraud Detection, Zambia, Banking Governance

1. Introduction

The speed with which Financial Technologies (FinTech) have been adopted into the commercial banking sector has fundamentally changed the way financial institutions design, execute and monitor their internal control systems. FinTech covers a wide range of digital solutions, such as automated processing of transactions platforms, artificial intelligence (AI) based fraud detection, mobile banking, and real time data analytics. With banks increasingly relying on these technologies to address risk management and regulatory compliance, as well as to enhance operational efficiency, questions are being raised about the degree to which the integration of FinTech is actually helping to maximize the effectiveness of internal controls.

The historical development of the internal control in global banking has been altered to include a more holistic, technology-based system of risk management, as opposed to a very narrowly-focused and clerical-focused system of internal control. In the past, the siloed aspect of the traditional internal control (mostly manual and reactive) was not sufficient to respond to the sophisticated financial crime and market volatility. The failures of high profile institutions such as the collapse of Credit Suisse and other global banking scandals highlighted how traditional controls were usually subject to execution risk and human judgment failures as manual overrides and slow reporting enabled illicit actions to go unnoticed (Muchiwa, 2021). According to Arwinge (2013), the character of the control activities has changed into a globally established COSO and Basel framework particularly to deal with the information asymmetry and moral hazard in the financial institutions.

FinTech was one of the calculated reactions to these deficiencies of control in the global environment. According to academic discourse, the necessity to reduce managerial discretion and improve the monitoring aspect of internal control was the main factor that led to the implementation of FinTech (Banna et al., 2021). Before this digital transformation, banks had problems with real time controls but the implementation of Artificial Intelligence (AI) and blockchain has added automated discipline to banking systems. Chen et al. (2022) found that FinTech is a governance capable of relevance that enhances internal control, through its capability to generate immutable audit trails and predictive risk identification unattainable with manual systems.

FinTech adoption in Sub Saharan Africa, and Zambia in particular, has been increasing at a faster rate in the last few years, due to financial inclusion demands, competition, and regulatory support. The number of digital financial transactions in Zambia has increased by more than 70 percent in the past four years between 2018 and 2022 (PwC Zambia, 2022), but studies have shown that the internal controls of Zambian commercial banks are mostly based on traditional mechanisms that might not be sufficiently effective to manage the dangers posed by digital platforms (Mwale and Habaazoka, The literature on the influence of FinTech on internal controls in this regard is therefore scant, with most of the available literature being devoted to financial performance, risk taking behaviour or digital adoption patterns as opposed to the internal control environment as a multidimensional governance construct.

This paper fill this gap by exploring how FinTech can be used to improve the effectiveness of internal controls in the context of Indo Zambia Bank (IZB), a commercial bank in Lusaka, which has made significant digital transformation efforts. This paper evaluates FinTech-based solutions implemented by the bank, the connections between integrated FinTech solutions and the effectiveness of internal controls, and how the bank personnel view the role of FinTech in internal control activities.

1.2 Statement of the Problem

The banking sector introduced Financial Technologies, which have been found to increase efficiency in operations, better customer service delivery, and enhanced internal controls by automating the monitoring process, reducing human error, and enhancing real time fraud and anomaly detection (Arner et al., 2015). It is preferable that banks should incorporate FinTech applications, including AI-based risk analytics, automated transaction monitoring, and digital audit trails into their internal controls, which will enable them to identify irregularities in time, enhance risk governance, and enhance financial reporting integrity (Liu et al., 2025). In the digital banking context (high volumes of transactions and greater complexity of operations), robust internal control frameworks are especially important to protect financial assets, ensure compliance, and retain confidence of stakeholders (Hamed, 2023).

This expectation was not the case as evidence indicates that numerous banks, such as those in Sub Saharan Africa and Zambia, have been struggling greatly to successfully incorporate FinTech into internal control systems. Cybercrime has become a more common occurrence around the world, and the number of cyberattacks on financial institutions has grown by 238 percent over the past two years (2020 to 2022) (Gulyás and Kiss, 2023; Patidar and Sen, 2022), which points to the inefficiency of digital transaction protection and real time monitoring tool. Current research in Zambia has shown that FinTech implementation can enhance financial performance and operational efficiency, though it offers limited empirical research investigations of how FinTech architectures are associated with particular internal control elements including the control environment, risk assessment, control activities and internal audit functions (Kasonde and Yohane, 2025; Kawimbe et al., 2025). Lack of these weaknesses subjects banks to operational, financial and reputational risks such as undetected fraud, misleading financial reporting, and regulatory fines, that may erode consumer confidence and the stability of the financial sector as a whole.

The implication is that policymakers, bank management, and regulators do not have institution level evidence to inform decisions regarding FinTech regulation and internal control investment in the Zambian banking sector. This is where this study comes in answering this evidence gap.

1.3 Objectives

The study was guided by three specific objectives:

- To explore the FinTech solutions adopted by Indo Zambia Bank.
- To assess the relationship between integrated FinTech systems and internal control effectiveness at Indo Zambia Bank.
- To explore the perceptions of bank staff regarding the effectiveness of FinTech tools in enhancing internal control processes.

2. Literature Review

2.1 Theoretical Framework

Technology Acceptance Model (TAM)

This study draws on Davis's (1989) Technology Acceptance Model (TAM), which posits that perceived usefulness and perceived ease of use are the primary determinants of individuals' intentions to adopt and use technology. TAM has been especially adapted to study the adoption of FinTech in banking, as the success of internal controls does not solely hinge on the technical functionality of deployed systems, but also on the degree to which personnel do not simply adopt them in a token manner. The perception of the usability and utility of FinTech used positively influence the adoption rate,

which subsequently predetermines the provision of governance and control advantages of these systems. In areas where employees feel FinTech applications cumbersome, hard to use, or of little practical use, adoption quality is negatively affected, and internal control benefits are limited. The application of TAM to the relationship between technology deployment and control effectiveness applies FinTech tools staff acceptance and utilisation as a mediating variable.

Control Theory

The governance perspective of this study is Control Theory, which is based on the studies of Arwinge (2013) and the COSO (2023) Internal Control Integrated Framework. COSO framework recognizes five elements of effective internal control that are interrelated and they include the control environment, risk assessment, control activities, information and communication, and monitoring activities. In this analysis, these elements are implemented to evaluate the interaction and reinforcement of each aspect of internal control system by FinTech tools in Indo Zambia Bank. The Agency Theory also serves to supplement this view by pointing out that digital monitoring technologies have the potential of minimizing information asymmetry between principals (bank management and regulators) and agents (operational staff) and enhancing accountability and minimizing risk of fraudulent conduct (Jensen and Meckling, 1976). In combination, TAM and Control Theory offer a conceptual architecture, which connects FinTech adoption behaviour with governance outcomes.

2.2 Empirical Review

Global Evidence

FinTech integration globally has been proven to enhance the quality of internal controls and lower institutional risk taking. Using a sample of Chinese listed banks, He et al. (2023) show that greater FinTech adoption is linked to an improved internal control quality and reduced risk taking in banks, and that digital technologies increase transparency and improve monitoring mechanisms. On the same note, Li et al. (2022) demonstrate that FinTech innovation helps to mitigate risk taking by enhancing capital adequacy and enhancing risk control capabilities, however, to a larger degree in bigger, more institutionally-potent banks. These results indicate that the magnitude and maturity of FinTech governance infrastructure mediates control benefit strength.

The literature attributes governance structures as key intermediaries of control benefits of FinTech. Ferilli et al. (2024) posit that FinTech usage can only increase the performance and stability of a system when there are structured governance bodies in place, and that the absence of consistent control over the system through coherent oversight can result in weakening of control systems instead of strengthening them due to technological integration. This conditionality view is consistent with Liu et al. (2025), who show that compliance systems based on AI may produce false positives and monitoring burnout in the absence of proper human supervision and interpretive governance systems.

Global literature also contains a lot of information about the risk dimensions of FinTech adoption. Lee and Shin (2018) single out the efficiency risk paradox, when the efficiency benefits of FinTech are compensated by the increased vulnerability to digital fraud and cyber threats. Mabe and Simo-Kengne (2025) also show through a Panel Vector Autoregression (PVAR) framework across African banks that FinTech risk significantly impacts negatively on bank performance, which highlights the two-sidedness of digital banking transformation. Appiah and Agblewornu (2025) further posit that perceived risk, perceived benefit, and trust are the key elements of sustained FinTech adoption, with cybersecurity trust becoming a determining factor in banking in Sub Saharan Africa.

Sub Saharan African Evidence

The movement of internal control has been characterized in Sub Saharan Africa through a shift in bureaucratic rigidity to digital agility. Over time, most African banking industries have been typified by poor culture of control and high rates of operational fraud as well as lack of enforced regulation (Ofoeda et al., 2023). The implementation of FinTech in Africa and especially hubs such as Kenya, Nigeria and South Africa was to jump over these institutional weaknesses. Research shows that in African markets with low levels of external enforcement, FinTech can be used as a governance complement, which replaces dysfunctional external enforcement by automating compliance processes (Djoufouet and Pondie, 2023). Yet, this fast implementation has also created cyber resilience risks, as now digital controls are required to protect against more advanced external threats.

Chinoda and Kapingura (2024) discover that partial or incomplete integration with FinTech can be more susceptible to operations, whereas more systemic integration reinforces internal controls. This difference between superficial digitisation and structural FinTech integration is especially true in the case of Zambian commercial banks, where the uptake of technology has in many cases outpaced the governance structures required to sustain them. Banna and Alam (2021) show that ASEAN banking digital financial inclusion leads to systemic stability, but warn that this effect needs to be supported by strict regulatory controls to avoid the development of fragility due to the rapid pace of digitalisation.

Zambian Evidence

In Zambia, available evidence confirms that FinTech enhances financial inclusion and operational efficiency but points at structural limitations to the realisation of the benefits of full internal control. Kasonde and Yohane (2025) note that the adoption of FinTech is limited by infrastructure, cybersecurity and implementation expenses, and that technological investments do not necessarily result in better governance results with ineffective internal systems and employee skills.

Kawimbe et al. (2025) go further to note that digital platforms have increasingly emerged as focal points of transactional efficiency, but governance alignment and digital literacy stand out as major gaps in Zambian commercial banks.
Mwale and Habaazoka (2023) are extremely informative as they show that the internal control systems continue to play a central role in mitigating risk in the Zambian commercial banks and that the effectiveness of control structures is strongly related to the reduction in the risks. This observation determines the governance interests of successful FinTech deployment within the Zambian banking context. Kawimbe and Kwalombota (2024) also show that cybersecurity threats have become a central issue in digitisation of banking processes in Zambia, and the increasing attack surface of digital platforms necessitates proactive, as opposed to reactive, risk management approaches. Mukuka and Qutieshat (2025) also mention digital literacy gap as one of the key limitations to the benefit of internal control of FinTech in the banking sector of Zambia, citing the central nature of human capital investment and implementation of technology.
The literature reviewed demonstrates that FinTech is capable of increasing monitoring capacity and the quality of internal control but the relationship is conditional based on the alignment of governance, institutional capacity, and development of human capital. The research is an addition to the evidence base by offering institution level, empirically based research on the impact of FinTech systems on internal control effectiveness in a Zambian commercial bank, where a gap in the contextual literature persists.

3 Research Methodology

3.1 Research Philosophy and Design

The research philosophy used was pragmatic and convergent parallel mixed method design, where quantitative surveys and qualitative interviews were carried out simultaneously and combined in the course of analysis (Creswell and Creswell, 2023). The epistemological orientation chosen was pragmatism since this orientation places more emphasis on practical problem solving than sticking to one paradigm, where the researcher was able to use the best of both approaches concluding with a quantitative measure and qualitative richness without philosophical antagonism. The convergent parallel design allowed to triangulate the results and get an in-depth insight into the statistical relationship between the constructs of FinTech and internal control as well as the lived experiences and perceptions of employees who interacted directly with these systems.
Quantitative methods enabled the measurement of the correlational relationships between the FinTech constructs and internal control effectiveness in a representative sample, whereas qualitative methods enabled the exploration of the contextual factors, such as the implementation challenges, the perception of cybersecurity risks, the adequacy of training, and governance gaps, which could not be exhaustively assessed with the help of quantitative instruments. Integration happened at the interpretation level, in which quantitative results were interpreted through the prism of qualitative themes and the other way around, resulting in a more coherent and practical analysis than either of the methods could have offered alone.

3.2 Population, Sampling and Study Site

The research took place in the case of Indo Zambia Bank (IZB), Lusaka, focusing on employees working in the compliance, internal audit, risk management, and digital operations departments. The research site was chosen as IZB because it has a rich and a well-documented history of digital transformation, including the implementation of various FinTech systems throughout its core banking, transaction processing, and compliance activities. The technological intensive nature of the operational environment of the bank offered a perfect institutional setting in which the relationship between the adoption of FinTechs and internal control effectiveness could be studied.
Since the population size in the various departments of interest is unknown, the formula of Slovin was used with a margin of error of 8 percent to obtain an indicative sample of 156. The final number of staff members who took part in the quantitative survey was 140, and it was 89.7% response rate. Stratified random sampling was used to have proportional representations in departments, levels of seniority, and operational roles. In the qualitative part, ten key informants were purposely chosen among departments that have direct involvement in FinTech operations and internal control processes such as IT, compliance, internal audit, risk management, and digital operations. This intentional methodology provided that the qualitative data included the views of employees having substantial knowledge of the systems in question.

3.3 Data collection and analysis

A structured Likert scale questionnaire on FinTech adoption (automated monitoring systems, AI based fraud detection, and digital transaction platforms) and internal control effectiveness (procedural efficiency, reporting reliability and regulatory compliance support) was used to gather quantitative data. The tool was checked by the review of experts (academic and practitioner specialists) and tested on a pilot group to make sure that it is clear and reliable (Cronbachs alpha 0.7 or more in all constructs). Semi structured interviews with key informants were used to collect qualitative data using a thematic interview guide, which was achieved in accordance with the three objectives of the study. The interviews were held under a confidential environment, and audio-recorded with the permission of the participants who were then transcribed directly.
The analysis of qualitative data was performed with the help of descriptive statistics (means and standard deviations) and

Pearson correlation analysis in IBM SPSS Statistics. Thematic analysis was applied to the qualitative data based on a six-phase framework proposed by Braun and Clarke (2021) which included familiarisation of data, coding, theme development, review, naming and reporting. The University of Zambia Research Ethics Committee (UNZAREC) approved the ethical standards and all participants were informed of the ethical standards and gave informed consent before the study. Privacy of data, anonymity and voluntary responses were ensured

4 Results and Discussion

4.1 FinTech Solutions that Indo Zambia Bank has adopted

The research discovered that the Indo Zambia Bank had implemented a wide-ranging, multi-layered portfolio of FinTech solutions in terms of customer facing, transactional, and compliance roles. The Flexcube platform and Oracle Financial Crime Compliance (Oracle FCC) software were the cornerstones of core banking operations. RTGS (Real Time Gross Settlement), DDACC (Direct Debit and Automated Clearing Centre) and the Postilion Switch facilitated electronic funds transfer. Digital customer facing channels incorporated the IZB Mobile App, Indo Wallet, IZB NXT, and USSD banking that were backed by biometric authentication systems. Risk management and compliance functions were based on automated Anti Money Laundering (AML) monitoring tools, rule based alert systems, and transaction flagging systems embedded into the core banking infrastructure.

The quantitative results revealed that staff awareness of automated monitoring and reporting systems (M=4.12, SD=0.67), AI based fraud detection (M=3.91, SD=0.71) and digital transaction platforms (M=4.05, SD=0.64) was high. These average scores show that most of the staff felt that these systems were active and applicable to their operations. These findings were supported by qualitative data as key informants reported a technologically rich operating environment. KI1 (IT Officer Trainee) told me that the bank has automated fraud detection systems, transaction monitoring tools, AML systems, and rule based alert systems that are part of the core banking platform and provide real time monitoring, reported unusual transaction patterns, generate alerts of suspicious activities and maintain audit trails to review compliance.

Both the quantitative and qualitative data however showed the uneven depth of integration in the bank's FinTech environment. Transactional front-end systems and customer interaction systems were embedded within day-to-day operations but there was a clear lagging adoption of automation in back-end compliance reporting. Both KI2 (IT Officer) and KI7 (Compliance Officer) identified back-office systems not yet embedded into the digitally automated monitoring and this made some manual tasks necessary during the compliance reporting process. This patchy level of integration aligns with Kasonde and Yohane (2025) argument about integration gaps being key limitations to FinTech adoption in Zambian commercial banks and also the more general conclusion from Ferilli et al. (2024) that there needs to be structural not superficial FinTech integration for governance benefits to be achieved. The FinTech adoption type at IZB mirrors what Chinoda and Kapingura (2024) describe as a partial integration which may produce a hybrid control environment containing elements of both digital and manual processes and where elements of each may reduce, not enhance control reliability.

4.2 Strategies Practices

FinTech and Internal control effectiveness Relationship

The Pearson correlation analysis produced weak but positive significant associations between all the three FinTech variables and internal control effectiveness as shown in the correlation coefficients and significance levels in Table 1 below.

Table 1: Pearson Correlation: FinTech Constructs and Internal Control Effectiveness

FinTech Construct	Pearson r	Significance	Interpretation
Automated Monitoring and Reporting Systems	0.260	$p < 0.01$	Weak positive
AI Based Fraud Detection Systems	0.195	$p < 0.05$	Weak positive
Digital Transaction Platforms	0.291	$p < 0.01$	Weak positive

Source: Field Data (2026)

Digital transaction platforms had the strongest relation with effectiveness of internal controls ($r=0.291$, $p<0.01$), automatic monitoring and reporting systems the second strongest relation ($r=0.260$, $p<0.01$), and the relation between artificial intelligence based fraud detection systems and effectiveness of internal controls had the third highest relation ($r=0.195$, $p<0.05$). Overall, the mean of the internal control effectiveness was 3.85 (SD=0.62), which reflected neutral to favorable staff perception about their internal control. Improvement of process efficiency dimension had the strongest acceptance (M=4.01) and improvement of internal monitoring procedures had the lowest acceptance (M=3.70). Individual means for dimensions of internal control effectiveness are presented in Table 2.

Table 2: Descriptive Statistics: Internal Control Effectiveness Dimensions

Dimension	Mean	Std. Deviation	Interpretation
Procedural Efficiency Improvement	4.01	0.58	Positive
Financial Reporting Accuracy	3.89	0.61	Moderately Positive
Regulatory Compliance Support	3.85	0.64	Moderately Positive
Anomaly Detection and Alerting	3.78	0.69	Moderately Positive
Internal Monitoring Strengthening	3.70	0.72	Moderate
Overall ICE Score	3.85	0.62	Moderately Positive

Source: Field Data (2026)

These findings are supported by He et al. (2023) and Li et al. (2022), who establish a positive correlation of FinTech adoption and the internal control quality in Chinese banks, but also, the authors confirm that the effectiveness of these relationships depends on the institutional capacity and governance systems. The low correlations at IZB indicate that, although FinTech tools were actively used and positively viewed, the effects of their governance were limited by the lack of system integration, the limited ability to proactively detect fraud, and the inconsistency of staff FinTech literacy levels, which does not allow the complete translation of digital capability into the effectiveness of control.

This picture was immensely enriched with qualitative evidence. KI1 explained how the automated AML systems, real time transaction monitoring and biometric authentication had enhanced the control environment of the bank. KI6 (Officer, 24 years) observed that, since the implementation, fraud monitoring had helped to reduce the number of incidents detected. But KI4 (Graduate Trainee) pointed to a major weakness: fraud detection was more reactive, and most cases were detected after the damage was done instead of fraud being prevented in the first place. This reactive stance indicates the distance between the operational implementation of FinTech and its complete implementation into governance-based internal control framework - the difference that the weak correlations statistically verify.

The conditionality thesis is also backed by the observation that digital transaction platforms which is the most widely adopted and operationally embedded FinTech element at IZB produced the most significant association with internal control effectiveness. The given pattern indicates that the depth of adoption and integration of governance are considered to be two important moderators of the FinTech control relationship, which empirically supports the argument by Ferilli et al. (2024) that coherent governance structures are the conditions under which the benefits of FinTech control can be realised.

4.3 Discussion of Findings

FinTech Solutions that Indo Zambia Bank has adopted.

The general view of FinTech contribution to internal controls was mostly positive but subtle in various aspects among the staff. In all survey items, mean scores reflected moderate to-high levels of support of FinTech to enhance procedural efficiency (M=4.01), financial reporting accuracy (M=3.89) and regulatory compliance support (M=3.85). IT and compliance personnel had the most positive perceptions, as these staff members are more familiar with FinTech systems, and their understanding of their governance roles is more accurate. Operational employees were more unsure of the governance implications of FinTech tools, viewing them as operational and not control tools.

Qualitative data were thematically analyzed, and five themes were identified, which intersect to describe the dimensions of staff experience with FinTech at IZB: perceived benefits, implementation challenges, cybersecurity threats, sufficient staff training, and improvement recommendations.

Theme 1: Perceived Benefits

Informants always emphasized that automation had decreased manual workloads, enhanced the accuracy of transaction monitoring and the reliability of audit trails. KI5 (Clerk, 6 years) highlighted that FinTech had enhanced operational security by use of controlled access systems, transaction verification measures and better monitoring measures that thwarted unauthorised activity. KI3 (Graduate Trainee) observed that automated monitoring systems had raised real time alerts, which has facilitated timely response, saving on time between the detection and escalation of an incident. These perceived benefits correspond to the quantitative result that an improvement in procedural efficiency was the most well-supported dimension of internal control effectiveness (M=4.01).

Theme 2: Implementation Challenges

Both quantitative and qualitative results found the implementation challenges as the moderating constraint to the benefits in control of FinTech. The most common challenge identified was back office integration gaps, with several informants indicating that processes in the company continue to be manual in areas where automation in digital format should have applied. KI2 (IT Officer) pointed out that difficulties with vendor engagement such as situations where the vendors were

inadequately skilled technically had contributed to delays in implementation and inefficiency in their operations. This vendor competency risk adds another level of vulnerability because the effectiveness of the internal control of IZB will be partially reliant on the competence and steadiness of external technology vendors.

Theme 3: Cybersecurity Risks

The issue of cybersecurity threats became a crosscultural and highly personal issue among all ten key informants. According to KI2 (IT Officer), all systems have a general susceptibility to cybersecurity risks, whereas KI1 recognized data breaches, phishing, and malware as ongoing operational risks that need to be mitigated constantly. The human factor was identified in KI4 (Graduate Trainee) as a key weakness since customers who reveal confidential information like personal identification numbers are a thorny and hard to-manage threat. KI5 (Clerk) cited that digital scamming is an increasing issue as criminals take advantage of digital platforms more often. Firewalls, encryption technologies, multi factor authentication, regular security audits, staff awareness training, and disaster recovery planning are the current mitigation strategies in the bank (KI1).

These results are consistent with the study of cybersecurity as an emerging risk in commercial banking in Zambia by Kawimbe and Kwalombota (2024) and the global efficiency risk paradox described by Lee and Shin (2018), in which operational efficiency benefits due to FinTech are offset systematically as the organization becomes more exposed to digital fraud and cyber threats. The apparent agreement on the risk of cybersecurity between all informants at IZB highlights the importance of cybersecurity preparedness as a core, non-negotiable element of FinTech regulation and not a peripheral issue.

Theme 4: Adequacy of Staff Training

Adequacy in training was found to be an important moderator of the effectiveness of internal controls of FinTech. KI4 stated that the role of governance of FinTech was not clearly comprehended by staff since online training was less interactive and engaging compared to physical programmes, and staff had to use user manuals instead of internalised knowledge of the system. KI1 pointed out that some personnel needed more training to recognize control capabilities of FinTech tools beyond operational utility, and there was a lack of awareness of the presence of systems and control intention. KI6 (Officer, 24 years) emphasized that external training to be offered by the specialist organizations like ZICTA led to positive outcome in the staff competency, implying that the training gap can be bridged by incorporating external training with internal training in terms of professional development programmes.

This observation is in line with Mukuka and Qutieshat (2025) finding that digital literacy gaps are an obstacle to the internal control benefits of FinTech in Zambian banking, and with TAMs prediction that perceived ease of use, and is increased by effective training, is a key determinant of the quality of technology utilisation. In cases where the staff training is deficient, the FinTech systems can be utilized in small or procedural scopes that can only get a fraction of the governance value.

Theme 5: Vendor Management

The dimension of vendor competency and governance oversight turned out to be another source of risk that has a direct impact on internal control effectiveness. According to KI2, contracting vendors with poor technical capabilities had led to delays in implementation, technical configuration mistakes and inefficiencies in operations that temporarily undermined the control processes. This observation is a governance blind spot that is not sufficiently covered by IZB existing FinTech management framework: the degree to which the effectiveness of its internal control relies on third party technology providers, which might not be subject to sufficiently strong oversight. This vulnerability must be sealed by vendor governance frameworks that outline technical due diligence criteria, performance service level agreements and incident response policies.

5 Conclusions and Recommendations

5.1 Conclusions

In this study, the authors presented empirical data that the adoption of FinTech in Indo Zambia Bank has positively, but insignificantly, increased the effectiveness of internal control in three main governance areas, such as procedural efficiency, financial reporting accuracy, and regulatory compliance support. The bank has a wide and actively running FinTech portfolio, but the level of integration is not even, with the back-office compliance automation much behind well embedded front end transactional systems.

Empirical evidence of the conditionality thesis that the addition of FinTech to governance is not automatic, but rather contingent on complementary governance structures, completeness of system integration, staff competency, and cybersecurity preparedness is found in the positive and weak correlations between FinTech constructs and internal control effectiveness (r=0.195 to r=0.291). This observation is consistent with and builds on the international literature by offering institution level data of a commercial bank in Zambia or any given context, which has been less represented in the empirical literature on digital banking governance.

The staff perceptions were generally positive, especially around procedural efficiency and accuracy of reporting, but were always tempered with cybersecurity risk awareness, the belief that fraud detection was reactive instead of proactive, and inconsistent training across staff levels and departments and uncertainties over the governance role of FinTech tools beyond its utility in detection. These perception patterns suggest that IZB has already integrated FinTech into its operational culture but has not yet attained the deeper governance integration in order to turn digital ability into more tangible and more powerful internal control results.

The results of the study add to the existing research on the governance of digital banking in developing economies by offering institution level evidence that does not rely on performance proxies but directly measures the quality of control outcomes. The conditionality framework that this research proposes, conditionality gains of FinTech is a factor of control alignment, depth of integration, staff capacity and cybersecurity preparedness is a practically actionable frame to bank management, regulators, and policymakers to optimise FinTech investment to yield governance benefits.

5.2 Recommendations

For Indo Zambia Bank Management

The bank also should focus on the complete automation of back-office compliance with its current digital environment, such as aligning financial reporting systems with core banking platforms to remove the need to have manual intervention in compliance reporting processes. This integration must be approached as a strategic governance priority as opposed to a technical exercise with a clear accountability to senior management on timelines of delivery and performance.

Predictive analytics and machine learning-based anomaly detection tools should be strengthened to allow proactive fraud detection before any losses occur, rather than raising a red flag afterwards. An organised employee training program in FinTech governance, cybersecurity, and internal audit roles in online settings must be institutionalised, with both online and physical mandatory elements to overcome the engagement gap found by informants. The vendor governance models must be formalised and must have technical due diligence, performance service level agreement, and incident response guidelines to the third-party technology providers.

To Commercial Banks in Zambia.

Adoption of FinTech is a governance/control strategy and not an exercise of operational efficiency. Investments in technologies must be matched by investments in governance structures, risk management capabilities, and human capital in order to make sure that the implementation of the FinTech will be translated into the quantifiable changes in the effectiveness of internal control. Banks must implement phases of implementations where they can test properly, familiarize their staffs and also ensure that their implementation is validated by their regulatory bodies before complete implementation.

Strong cybersecurity risks management systems such as sophisticated threat detection systems, multi factor authentication tools, data encryption, and incident response strategies should be integrated as a constitutive element of the digital banking systems. Another control weakness that banks should invest in in digital banking environments is sector wide digital literacy programmes to digitally equip staff and customers to limit human vulnerability.

To the Bank of Zambia.

Bank of Zambia ought to prepare and release an inclusive FinTech explicit regulatory framework that sets out minimum internal control requirements regarding digitally integrated banking operations. Such a framework ought to support the system integration needs, cybersecurity requirements, vendor governance needs, and staff qualifications needs in the role of FinTech governance. The regulator must also provide supervisory guidance on automated monitoring and AI based tools of fraud detection, minimum performance standards of fraud detection rates, system uptime and timeliness of reporting. This would make sure that FinTech is implemented throughout the banking industry with demonstrable internal control enhancements and not cosmetic digitisation.

Policy Implications

This research has a number of policy implications to the governance of digital banking in Zambia. To begin with, it is not enough to invest in FinTech to ensure a better banking governance, organisational structures, human capital, and regulatory alignment should be tackled concomitantly. Second, there should be mandatory cybersecurity standards that will guarantee uniformity in risk mitigation among banks. Third, industry-wide education regarding FinTech governance needs to be adopted to enhance the capacity and knowledge of staff members regarding the digital control procedures. Fourth, digital literacy programmes should be included in financial inclusion efforts to safeguard customers and ensure access to digital financial services in a safe manner.

5.3 Limitations and Future Research

This study was subject to several limitations that should be considered in interpreting the findings. First, the study was

carried out at one institution, the Indo Zambia Bank which constrains the generalisability of the results to other commercial banks operating in various technological and organisational settings. Second, self reported Likert scale data carries the risk of social desirability bias, in which case the respondents could have rated FinTech adoption and effectiveness higher than they should have been based on the experience. Third, the qualitative sample of ten key informants, though purposely selected in terms of relevance, might not have reflected the entire scope of the perspectives at all the levels of the bank hierarchy. Fourth, data collection was cross-sectional, thus the study only captured perceptions at one point in time, and it cannot be used to explain the changes in FinTech integration or internal control effectiveness across time. Fifth, due to the correlational design, no causal conclusions can be drawn regarding the direction or the magnitude of the impact that FinTech can have on the internal control outcomes.

Longitudinal designs that trace the evolution of internal control effectiveness with the further development of FinTech integration should be considered in the future research to address these constraints. The multi bank studies on Zambia would allow cross institutional comparison and generate findings that are more generalisable. To test the mediation and moderation of the FinTech control relationship through governance structures, the cybersecurity capacity and the competency of the staff, structural equation modelling or regression based approaches are to be used. Additional insights on customers side such as digital literacy, fraud experiences, and attitudes towards digital security should be investigated to supplement institutional perspectives portrayed by this research.

Declaration of Competing Interests

The authors declare that they are not aware of any competing financial interests or personal relationships that may have influenced the work described in this document.

Funding

This research did not receive specific grants from any public, commercial, or non-profit sector funding bodies.

Acknowledgements

The author would like to offer my heartfelt gratitude to everyone who made a contribution to this research

Ethical considerations

The article followed all ethical standards appropriate for this kind of research.

References

Appiah, T. and Agblewornu, V.V. (2025). The interplay of perceived benefit, perceived risk, and trust in Fintech adoption: Insights from Sub Saharan Africa. Heliyon, 11, e41992.

Arner, D.W., Barberis, J.N. and Buckley, R.P. (2015). The Evolution of Fintech: A New Post-Crisis Paradigm? SSRN Electronic Journal.

Arwinge, O. (2013). Internal Control: A Study of Concept and Themes. Physica-Verlag HD, Heidelberg.

Banna, H. and Alam, M.R. (2021). Impact of digital financial inclusion on ASEAN banking stability: implications for the post Covid 19 era. Studies in Economics and Finance, 38, 504–523.

Braun, V. and Clarke, V. (2021). Thematic Analysis: A Practical Guide. SAGE Publications.

Chinoda, T. and Kapingura, F.M. (2024). Digital financial inclusion and economic growth in Sub Saharan Africa: the role of institutions and governance. African Journal of Economic and Management Studies, 15(1), 15–30.

COSO (2023). Internal Control — Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission.

Creswell, J.W. and Creswell, J.D. (2023). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications.

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319–340.

Djoufouet, W.F. and Pondie, T.M. (2023). Financial technology and financial inclusion in sub Saharan Africa. Journal of Risk and Financial Management, 16(11), 472.

Ferilli, G.B., Palmieri, E., Miani, S. and Stefanelli, V. (2024). The impact of FinTech innovation on digital financial literacy in Europe: Insights from the banking industry. Research in International Business and Finance, 69.

Gulyás, L. and Kiss, G.D. (2023). The cybersecurity vulnerability of critical financial infrastructure. Public Finance

Quarterly, 68(1), 27–42.

He, M., Song, G. and Chen, Q. (2023). Fintech adoption, internal control quality and bank risk taking: Evidence from Chinese listed banks. Finance Research Letters, 57, 104235.

Jensen, M.C. and Meckling, W.H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.

Kasonde, C. and Yohane, R. (2025). Evaluating the Effect of Financial Technologies and Agency Banking on the Financial Performance of Selected Commercial Banks in Zambia. African Journal of Management and Business Research, 20, 217–234.

Kawimbe, S. and Kwalombota, M. (2024). Mitigating Cybersecurity Risks in the Digitization of Banking Operations: Strategies, Challenges, and Best Practices for Zambian Commercial Banks. International Journal of Research and Innovation in Social Science, VIII, 2988–3005.

Kawimbe, S., Mweemba, B. and Mukosa, F. (2025). An Appraisal of the Impact of Financial Technologies (FinTechs) on Financial Inclusions in Selected Parts of Zambia. International Journal of Finance, 10, 54–74.

Lee, I. and Shin, Y.J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. Business Horizons, 61(1), 35–46.

Li, C., He, S., Tian, Y., Sun, S. and Ning, L. (2022). Does the bank's FinTech innovation reduce its risk taking? Evidence from China's banking industry. Journal of Innovation and Knowledge, 7, 100219.

Liu, Y., Wang, R. and Zhang, L. (2025). AI driven compliance and governance risk in digital banking: a systematic review. Journal of Financial Regulation, 11(1), 45–68.

Mabe, Q.M. and Simo-Kengne, B.D. (2025). The Impact of Fintech Risk on Bank Performance in Africa: The PVAR Approach. Journal of Risk and Financial Management, 18, 456.

Mukuka, A. and Qutieshat, A. (2025). Digital transformation and strategic challenges in Zambian banking: Systematic review.

Mwale, A. and Habaazoka, L. (2023). A Study on the Effectiveness of Internal Control System on Commercial Banks Risk Minimization in Zambia. European Modern Studies Journal, 7, 147–162.

Muchiwa, M. (2021). Internal audit effectiveness and corporate governance in financial institutions. Zambia Journal of Business Studies, 3(1), 12–28.

Ofoeda, I., Gariba, P. and Aboagye, A.Q.Q. (2023). Non bank financial institutions regulation, governance and performance. Journal of Financial Regulation and Compliance, 31(1), 31–52.

Patidar, A. and Sen, S. (2022). Cybersecurity threats to financial institutions: patterns, impacts and countermeasures. International Journal of Information Security and Privacy, 16(1), 1–18.

PwC Zambia (2022). Digital financial services in Zambia: Growth, opportunities and risks. PricewaterhouseCoopers Zambia Report