****

**DOI:** <https://doi.org/10.38035/dar.v2i4>

<https://creativecommons.org/licenses/by/4.0/>

**Internal Control System and the Use of Digital Applications as an Effort to Prevent Fraud in Financial Institutions (A Conceptual Study and Guide for Researchers)**

**Agostinho Coelho1 & Susi Artati2**

1Universidade Oriental Timor Lorosa’e, Dili, Timor Leste, email: agostinhocoelho77@gmail.com

2Universitas Batanghari, Jambi, Indonesia, email: susiartati30@gmail.com

Corresponding Author: susiartati30@gmail.com1

**Abstract:** This study aims to conceptually examine the role of internal control systems and the use of digital applications as efforts to prevent fraud in financial institutions. The increasingly complex and sophisticated nature of fraud requires financial institutions to enhance their monitoring and control strategies. This paper presents a review of relevant literature and theories regarding internal control and digital transformation in detecting and preventing fraud. The findings indicate that an effective internal control system—which includes the control environment, risk assessment, control activities, information and communication, and monitoring—has a significant impact on reducing the likelihood of fraud. Meanwhile, the integration of technology through digital applications adds value by enabling easier transaction monitoring, real-time data tracking, and strengthening technology-based audit systems. This article is expected to serve as a conceptual guide for researchers in developing further studies related to fraud prevention in the digital era, particularly in the financial sector.

**Keyword:** Internal Control Systems, Digital Applications, & Fraud

# INTRODUCTION

In an increasingly complex digital era, financial institutions face significant challenges related to the growing risk of fraud, which has become more sophisticated and harder to detect. While advancements in information technology bring operational efficiency, they also create opportunities for criminals to exploit financial systems. According to Musyoki (2023), fraud in the financial sector can lead to substantial financial losses, legal consequences, and a decline in stakeholder trust.

The internal control system (ICS) is a vital mechanism in the prevention and detection of fraud. An effective ICS encompasses control environment, risk assessment, control activities, information and communication, and monitoring. Research by Musyoki (2023) indicates that a strong ICS plays a crucial role in ensuring the accuracy of financial reporting and preventing fraud. Furthermore, Saputra & Rosharlianti (2025) also show in their study that ICS, along with internal audits and good corporate governance, has a significant influence in preventing fraud in non-bank financial institutions. This underscores that ICS is not merely an administrative tool but also a fundamental pillar in maintaining integrity and trust in the financial sector.

ICS plays a crucial role in preventing fraud within financial institutions. It is designed to reduce the likelihood of fraud by implementing strict policies and procedures, as well as clear segregation of duties among employees. In this way, the ICS helps ensure that no single individual has complete control over all aspects of financial transactions, thereby reducing the risk of abuse of authority (New York State, 2025).

The importance of strengthening the ICS has also been emphasized by the Otoritas Jasa Keuangan (OJK) as an effort to minimize the risk of fraud. OJK recommends the implementation of an anti-fraud strategy that includes prevention, detection, investigation, and follow-up—each of which relies heavily on a strong ICS (OJK, 2024). Moreover, an effective ICS enables early detection of suspicious activities, allowing organizations to take corrective action before significant losses occur. ICS also contributes to improved operational efficiency by identifying and correcting unnecessary or weak procedures within the system (Bwerinofa-Petrozzello, 2023).

In addition to the ICS, the integration of digital technology within internal controls is becoming increasingly important in addressing the growing threat of fraud. The use of digital applications enables real-time transaction monitoring, big data analysis, and the detection of anomalous patterns that may indicate fraudulent activities. According to Tookitaki (2024), platforms such as FinCense utilize advanced technologies to effectively detect and prevent fraud by combining real-time monitoring with collective analytics.

The use of digital applications is considered to play a crucial role in fraud prevention efforts within financial institutions, especially in this era of rapid digital transformation. The integration of advanced technologies such as artificial intelligence (AI), machine learning, and federated learning has proven to enhance the effectiveness of internal control systems in detecting and preventing increasingly complex fraudulent activities.

However, the implementation of digital technology in fraud control also faces challenges, such as the need for transparency, data privacy, and the avoidance of bias in detection models. Awosika et al. (2023) emphasize the importance of using Federated Learning and Explainable AI to ensure that fraud detection systems are not only effective but also trustworthy and respectful of user privacy.

In recent years, financial institutions have increasingly relied on digital technology in their operations, such as mobile applications, online banking services, and other digital transactions. While this technology enhances efficiency and accessibility, it also opens gaps for increasingly sophisticated fraud threats. Therefore, research examining how digital applications can be used to detect and prevent fraud is highly relevant.

Fraud in financial institutions continues to evolve, both in terms of techniques and scale. Technologies such as ransomware, phishing, and cyber-attacks are increasingly used by criminals to undermine the integrity of financial systems. An effective ICS, combined with digital applications that can detect and prevent fraud, has become more crucial than ever.

Regulations regarding fraud prevention and data security are becoming increasingly strict, both at the national and international levels. Financial institutions must comply with better internal control standards to prevent fraud and ensure compliance with applicable regulations, such as those set by the OJK or other regulatory bodies. This research is relevant because it can provide guidance for researchers and practitioners to develop or update policies and procedures in financial institutions.

This research is also important because it provides insights into the integration of technology in internal control systems. Technologies such as AI, machine learning, and blockchain can enhance the ability of financial institutions to detect and prevent fraud more efficiently and accurately. Research on digital applications that can be used in internal control systems is an increasingly developing and urgent topic.

With the rapid technological changes, financial institutions require up-to-date guidance on the implementation of ICS and digital technologies to prevent fraud. This research makes an important contribution by providing a conceptual study that can serve as a guide for researchers and practitioners to develop more adaptive and technology-based internal control systems.

This article aims to provide a conceptual review of the role of internal control systems and digital applications in fraud prevention within financial institutions. By reviewing the latest literature and best practices, this article is expected to serve as a guide for researchers and practitioners in developing effective fraud prevention strategies in the digital age.

# METHOD

This study uses a qualitative approach with a conceptual study method, aimed at deeply examining the theories, concepts, and empirical findings related to internal control systems (ICS) and the use of digital applications in fraud prevention within financial institutions. This method allows the researcher to develop a comprehensive conceptual framework as a guide for future research.

Data collection was conducted through library research, by reviewing relevant literature from academic journals, books, and research reports published in the past ten years. These sources were obtained from academic databases such as Google Scholar and Scopus, as well as repositories from higher education institutions.

Data analysis was conducted using content analysis, which involved identifying, categorizing, and synthesizing information from various sources to develop a deep understanding of the role of internal control systems (ICS) and digital applications in fraud prevention. This approach allows the researcher to identify patterns, relationships, and gaps in the existing literature, as well as to construct a conceptual framework that can serve as a foundation for future empirical research.

To ensure the validity and reliability of the findings, this study uses source triangulation by comparing information from various types of publications and perspectives. Additionally, the researcher also considers both local and global contexts in the analysis to ensure that the developed conceptual framework is relevant and applicable in different situations.

# RESULTS AND DISCUSSION

**Internal Control System as an Effort to Prevent Fraud in Financial Institutions**

Internal Control System (ICS) is a process designed and implemented by management and all personnel within an organization to provide reasonable assurance in achieving the organization's goals, particularly in terms of operational effectiveness and efficiency, reliability of financial reporting, and compliance with applicable laws and regulations. ICS includes policies, procedures, and practices applied to control risks and prevent deviations or fraud.

In the context of financial institutions, the Internal Control System (ICS) plays a crucial role in fraud prevention efforts. Fraud in the financial sector can involve asset misuse, financial statement manipulation, or other actions that harm the institution and its stakeholders. An effective ICS can help detect and prevent such actions through the implementation of principles such as task separation, transaction authorization, and stringent supervision.

According to OJK (2024), strengthening the ICS in financial service institutions is an important step to minimize the risk of fraud. OJK emphasizes that the complexity of business activities in financial institutions increases exposure to fraud risks, thus requiring a strong internal control system as part of risk management.

Furthermore, a good ICS not only serves as a preventive tool but also as an early detection mechanism for potential fraud. With effective internal controls in place, organizations can quickly identify and respond to indications of fraud, thereby reducing the negative impact that may arise (Bwerinofa-Petrozzello, 2023).

Ziorklui et al. (2024) in their study highlight that effective internal control mechanisms, such as advanced authentication techniques, monitoring suspicious activities, regular staff training, and strong data encryption, are crucial in identifying and preventing fraud in commercial banks. Additionally, Waromi et al. (2024) in their research show that ICS plays an important role in maintaining the integrity and reliability of financial information in the financial sector. Furthermore, several other studies by Fauziyah & Setyawan (2023); Widyawati (2019); Habibullah et al. (2024); and Pratopo & Wuryani (2023) also suggest that internal control systems have a positive and significant impact on financial systems.

However, the effectiveness of internal control systems (ICS) depends on their design and implementation. Research by Nugraha & Bayunitri (2020) emphasizes that failures in preventing fraud are often caused by both internal and external factors, including lack of training, ineffective supervision, and poor management practices.

In today’s digital era, the integration of information technology into internal control systems (ICS) is becoming increasingly important. The use of digital applications can enhance the effectiveness of internal controls through process automation, real-time transaction monitoring, and data analysis to detect suspicious patterns. This aligns with the need for financial institutions to adapt to technological developments and address new challenges in fraud prevention.

The integration of digital technology into internal control systems (ICS) also enhances their ability to prevent fraud. The use of digital applications enables real-time transaction monitoring and data analysis to detect suspicious patterns, thereby strengthening financial institutions' defenses against fraudulent threats.

Thus, internal control systems (ICS) are a crucial component in maintaining the integrity and stability of financial institutions. The effective implementation of ICS, supported by digital technology, can strengthen fraud prevention efforts and ensure operational sustainability as well as public trust in financial institutions.

**The Use of Digital Applications as a Fraud Prevention Effort in Financial Institutions**

Digital applications refer to software or information technology-based systems designed to perform specific functions through electronic devices such as computers, smartphones, or tablets. In the context of financial institutions, digital applications encompass various technological solutions used to support operations, including online banking systems, mobile banking applications, and analytical platforms for detecting suspicious activities.

The implementation of digital applications in the internal control systems of financial institutions has become crucial in efforts to prevent fraud. With the increasing complexity of financial transactions and the growing threat of cybercrime, digital technology offers the ability to monitor, detect, and respond to suspicious activities in real time.

According to the Financial Services Authority (OJK, 2024), strengthening internal control systems through anti-fraud strategies is essential to minimize the risk of fraud in financial institutions. This includes the implementation of information technology that can enhance the effectiveness of monitoring and early detection of potential fraud.

In addition, the use of technologies such as digital identity verification and the Zero Trust security model enables financial institutions to continuously verify user identities, thereby reducing the risk of unauthorized transactions or suspicious account activities (Preis, 2024). Furthermore, the implementation of digital applications also allows financial institutions to integrate various data and systems, thereby enhancing operational efficiency and the ability to detect unusual patterns that may indicate potential fraud.

One effective approach to leveraging technology, according to Preis (2024), is the use of digital identity verification. By utilizing digital identity solutions, banks can integrate fraud prevention strategies across the entire customer journey — from account creation to transaction execution. This enables holistic fraud detection and mitigation.

In addition, artificial intelligence (AI) has also become a powerful tool in detecting fraud. AI-based solutions can analyze large volumes of transaction data in real-time, identify suspicious patterns, and proactively mitigate threats. For example, the Appgate's Detect Transaction Anomaly (DTA) platform uses AI to review billions of transactions and prevent significant financial losses (Wilson, 2024).

However, it is important to strike a balance between fraud prevention and user experience. Technology can serve as a bridge to meet both of these needs, ensuring security without sacrificing user convenience (Henry, 2025). Thus, the integration of digital applications into the internal control system of financial institutions not only enhances operational efficiency but also strengthens defenses against increasingly sophisticated fraud threats. The implementation of this technology becomes a strategic step in maintaining integrity and trust in the financial sector.

# CONCLUSION

Fraud prevention in financial institutions is a significant challenge that requires a strategic and comprehensive approach. This study emphasizes that an effectively designed internal control system plays a crucial role in creating mechanisms for the prevention, detection, and mitigation of potential fraud. This system not only acts as a formal control but also serves as the foundation for building an organization’s integrity culture. On the other hand, advancements in digital technology have opened up great opportunities to support fraud prevention efforts through digital applications capable of monitoring transactions in real-time, detecting suspicious patterns, and automating early warning systems. The integration of internal control systems and the use of digital applications will strengthen financial security systems while improving operational efficiency and effectiveness in financial institutions. Therefore, this conceptual study is expected to serve as an initial guide for researchers and practitioners in developing adaptive fraud prevention models that respond to the dynamics of technology and modern financial challenges.

This study has important implications both theoretically and practically. Theoretically, it expands the understanding of the importance of integrating internal control systems with digital technology in preventing fraud in the financial sector. This implication serves as a foundation for future researchers to develop more comprehensive conceptual models, which not only focus on internal control aspects but also consider adaptations to technological advancements, particularly in the use of digital applications and artificial intelligence (AI).

Practically, the results of this study provide strategic input for policymakers in financial institutions to evaluate the effectiveness of existing internal control systems and encourage the adoption of digital applications as part of an integrated fraud prevention system. When used optimally, digital applications not only serve as monitoring tools but also act as intelligent and efficient early detection systems for suspicious transaction patterns.

In addition, for management and internal auditors, this study emphasizes the importance of training and improving digital technology literacy so that internal control processes are not conventional and static, but rather more adaptive to the challenges of the times. Thus, the implications of this study also encourage a shift towards a more proactive, transparent, and technology-based organizational culture in maintaining integrity and public trust in financial institutions.

**REFERENCE**

Awosika, T., Shukla, R. M., & Pranggono, B. (2023). Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection. arXiv

Bwerinofa-Petrozzello, R. (2023). Preventing fraud with internal controls: A refresher. *Journal of Accountancy.(*<https://www.journalofaccountancy.com/issues/2023/aug/preventing-fraudwith-internal-controls-a-refresher.html> *)*.

Fauziyah, A., & Setyawan, S. (2023). Pengaruh Penerapan Model Akuntansi Sektor Publik Dan Sistem Pengendalian Internal Terhadap Upaya Pencegahan Fraud. *Transekonomika: Akuntansi, Bisnis Dan Keuangan*, *3*(1), 23-31.

Habibullah, A. Z., Tarigan, J., Ibadurrahman, I., Kano, M. S., & Djasuli, M. (2024). Literature Review: Pengaruh Pengendalian Internal Terhadap Kecurangan (Fraud) Pada Laporan Keuangan Pemerintah Daerah. *Jurnal Ekonomi Revolusioner*, *7*(6).

Henry, J. (2025). How to Balance UX and Fraud in Digital Applications. <https://www.jackhenry.com/resources/articles/how-to-balance-ux-and-fraud-in-digital-applications?utm>

Musyoki, J. (2023). Internal Control Systems and their role in Financial Fraud Prevention in Kenya. ResearchGate

New York State. (2025). *Top Ten Internal Controls to Prevent And Detect Fraud*!. New York: Office of Mental Health.

Nugraha, R., & Bayunitri, B. I. (2020). The influence of internal control on fraud prevention (Case study at Bank BRI of Cimahi City). *International Journal of Financial, Accounting, and Management*, *2*(3), 199-211.

Otoritas Jasa Keuangan (OJK). (2024). Penerapan Strategi Anti Fraud Bagi Lembaga Jasa Keuangan.

Pratopo, R. D., & Wuryani, E. (2023). Pengaruh sistem pelaporan pelanggaran dan sistem pengendalian internal terhadap pencegahan kecurangan. *Journal of Economics and Business UBS*, *12*(3), 1707-1723.

Preis, A. (2024). How Digital Identity Powers Integrated Bank Fraud Detection, Response, and Prevention. <https://www.pingidentity.com/en/resources/blog/post/digital-identity-bank-fraud.html?utm>

Saputra, A. D., & Rosharlianti, Z. (2025). Pengaruh Pengendalian Internal, Audit Internal dan Good Corporate Governance terhadap Pencegahan Fraud. *AKADEMIK: Jurnal Mahasiswa Ekonomi & Bisnis*, *5*(1), 183-196.

Tookitaki. (2024). Comprehensive Guide to Fraud Prevention in Financial Institutions.

Waromi, J., Kambuaya, M. K., & Wonar, K. (2024). Evaluation of the Effectiveness of Internal Control Systems in Reducing Accounting Fraud in Financial Sector Companies. *The Eastasouth Management and Business*, *2*(03), 228-232.

Widyawati, A., Sujana, E., & Yuniarta, A. (2019). Pengaruh Kompetensi Sumber Daya Manusia, Whistleblowing System, dan Sistem Pengendalian Internal Terhadap Pencegahan Fraud Dalam Pengelolaan Dana BUMDES (Studi Empiris pada Badan Usaha Milik Desa di Kabupaten Buleleng). *JIMAT (Jurnal Ilmiah Mahasiswa Akuntansi) Undiksha*, *10*(3), 368-379.

Wilson, P. (2024). AI-Powered Fraud Prevention in Digital Banking Solutions. <https://www.appgate.com/blog/ai-powered-fraud-prevention-in-digital-banking-solutions?utm>

Ziorklui, J. E. K., Ampofo, F. O., Nyonyoh, N., & Antwi, B. O. (2024). Effectiveness of internal controls mechanisms in preventing and detecting fraud. *Finance & Accounting Research Journal*, *6*(7), 1259-1274.