



Adaptive Internal Controls and Digital Transformation in Preventing Public Sector Fraud

Galih Ganitama Putra¹

¹ Sekolah Tinggi Ilmu Ekonomi Surakarta, Sukoharjo, Indonesia

Abstract

Article history:

Received: January 4, 2024

Revised: February 15, 2024

Accepted: April 22, 2024

Published: June 30, 2024

Keywords:

Adaptive Internal Control,
Digital Internal Audit,
Digital Transformation,
Fraud,
Public Finance.

Identifier:

Zera Open

Page: 1-18

<https://zeraopen.com/journal/pp>

The development of the digital era has transformed the paradigm of public financial management through process automation, transaction digitalization, and cross-system data integration. This transformation creates significant opportunities for efficiency but simultaneously introduces new risks in the form of digital fraud and threats to the integrity of state finances. This study aims to analyze the role of adaptive internal control and digital internal audit in preventing fraud within the Indonesian public sector. By reviewing empirical literature from the last five years, the findings indicate that the implementation of digital audit tools, e-governance, and real-time internal control systems enhances accountability, early detection, and public financial transparency. Moreover, the digital competence of auditors and technology governance emerges as key determinants of the effectiveness of adaptive auditing in addressing cyber risks and digital fraud. Strengthening these elements contributes to building a resilient public financial oversight framework capable of responding to increasingly complex digital threats. The results of this study are expected to reinforce technology-based supervision policies and support the development of internal control systems that remain robust in the face of rapid digital advancement across government financial processes.



1. Introduction

Digital transformation has become a central pillar in the modernization of the public sector globally, including in Indonesia. The development of information technology has spurred the digitalization of government financial processes, encompassing planning, execution, reporting, and oversight of state finances. Through the implementation of e-budgeting, e-audit, and digital payment systems, the government strives to enhance bureaucratic efficiency, expand transparency, and strengthen public accountability. However, this rapid change also introduces new risks, particularly those related to data security, technology misuse, and the rise of complex, hard-to-detect digital fraud cases (Prasetyo, 2023).

In the context of public finance, digital risks significantly impact the effectiveness of auditing and internal control. The use of cloud computing, big data analytics, and automated accounting systems can accelerate the audit process, but simultaneously create new vulnerabilities for potential financial data manipulation. Research indicates that the increase in cyber fraud cases in the public sector has eroded public trust in government institutions and magnified the need for adaptive internal control systems (Rashid, 2022).

This shift in the risk landscape necessitates urgent reforms in government audit and oversight practices. Internal audit is no longer sufficient to merely focus on administrative compliance; it must also be capable of anticipating technology-based risks. Auditors in the digital era are required to possess competence in data analysis, understanding information systems, and the ability to detect fraud patterns through digital audit software. This aligns with the findings of Rosli et al. (2020),

who state that the digital competence of auditors and mastery of data-based audit technology have a positive relationship with the effectiveness of fraud prevention.

Furthermore, traditional internal control, which focuses on manual procedures, is deemed inadequate in facing cyber-based threats. An adaptive **internal control system** model is required to respond dynamically to changes through the integration of artificial intelligence, early warning systems, and real-time monitoring mechanisms. A study by Putri et al. (2023) confirms that organizations capable of adjusting their internal control systems to digital risks exhibit better resilience in preventing and detecting fraud than organizations with conventional approaches.

The phenomenon of digital fraud not only causes massive financial losses but also threatens the credibility of public institutions. Wibowo (2023) notes that the combination of weak internal control and low digital literacy among supervisory officials is often the main cause of failure to detect electronic-based transaction deviations. Therefore, enhancing human resource capacity is a crucial component in the fraud risk mitigation strategy in the digital era. Auditor technological competence and personal integrity play a vital role in building a highly competitive and transparency-oriented financial oversight system.

Furthermore, synergy between technology and good governance must be strengthened so that the internal control system functions not only as a detection tool but also as a strategic preventive measure. The implementation of a digital-based audit system offers the potential to continuously monitor transactions and identify anomalies early on (Ginanjari & Syamsul, 2020). However, without supportive policy

design, even sophisticated technology will not be effective in curbing malpractices. Therefore, digital transformation in government financial management must be accompanied by an increase in ethical culture, accountability, and risk-based oversight.

Thus, this research aims to examine the relationship between digital transformation, adaptive internal control systems, and fraud prevention in the public sector. This approach is expected to enrich the perspective on how the government can effectively manage digital risks through the implementation of technology-based internal audit and resilient adaptive control systems against cyber threats.

2. Literature Review

2.1. Digital Transformation in Public Financial Management

Digital transformation has been a primary catalyst for reform in public sector financial management across various countries, including Indonesia. The digitalization of accounting, reporting, and financial oversight processes has accelerated efficiency, reduced manual intervention, and expanded access to public financial data in real-time. According to Nurdin et al. (2019), the application of digital-based internal control systems is capable of strengthening the principles of good governance by increasing the transparency and accountability of state budget management.

The Indonesian government is gradually integrating systems such as e-budgeting, e-audit, and e-reporting to create technology-based financial governance. However, the adoption of digital systems also introduces new challenges in the form

of risks such as data leakage, manipulation of electronic transactions, and misuse of digital access. Wibowo (2023) emphasizes that financial digitalization without strong oversight can open new avenues for more sophisticated and hard-to-detect fraud. Therefore, strengthening institutional capacity in managing data and securing digital systems is an essential prerequisite for the success of public sector digital transformation.

Research by Rosli et al. (2020) indicates that the adoption of digital technology in public financial audit and management can increase examination efficiency, but its successful implementation is highly dependent on the digital literacy of auditors and managerial policy support. Without such support, digitalization only yields administrative efficiency without a genuine increase in the effectiveness of financial oversight. Thus, digital transformation in public financial management must be balanced with improving the quality of human resources, updating regulations, and strengthening adequate cybersecurity systems.

2.2. Adaptive Internal Control System

The Internal Control System (SPI) is a crucial mechanism for ensuring the reliability of financial reports, the effectiveness of operations, and compliance with regulations. In the digital context, the SPI concept evolves into adaptive internal control systems that can adjust to technological changes and the dynamics of cyber risks. Putri et al. (2023) affirm that public organizations implementing technology-based internal controls have a better ability to detect and prevent financial anomalies.

Adaptive SPI encompasses three key elements: automation of control procedures, integration of data analysis, and real-time monitoring mechanisms. With

the aid of technologies like data analytics and machine learning, auditors can identify unusual transaction patterns that potentially indicate fraud. Rashid (2022) show that public organizations implementing data-based controls experience a significant increase in the effectiveness of fraud detection compared to traditional methods.

However, the success of adaptive internal control systems is determined not only by technological sophistication but also by organizational readiness and the integrity of human resources. Prasetyo (2023) suggest that bureaucratic culture resistance to technological changes often hinders the optimal implementation of adaptive controls. Therefore, changes in work structure and continuous training for auditors are strategic steps in strengthening the effectiveness of internal control. The implementation of adaptive SPI also plays a critical role in building public trust in government institutions. When digital-based control systems are implemented consistently and transparently, the public will have greater confidence in the accuracy and honesty of state financial reports. Thus, adaptive SPI is not merely a technical tool but a core pillar in realizing public financial governance that is integrity-driven and resilient against digital risks.

2.3. Digital Internal Audit and Fraud Prevention

Internal audit has a strategic role in detecting and preventing financial fraud. In the digital era, the internal audit function evolves into digital audit, which is an audit process utilizing information technology and data analysis to identify potential deviations more quickly and accurately. Ginanjar and Syamsul (2020) explain that the use of digital audit technology, such as computer-assisted audit tools (CAATs) and continuous auditing systems, can shorten examination time and enhance the

effectiveness of abnormal transaction detection. Beyond speed, digital audit also expands the scope of oversight to areas previously difficult for manual auditors to reach. Putri et al. (2023) state that the integration between digital audit and strong internal control creates an effective synergy in preventing fraud, especially technology-based fraud like electronic data manipulation and digital fund diversion.

However, the transition to digital audit demands an increase in auditor competence, in both technical aspects and professional ethics. Wibowo (2023) highlights that the lack of data analysis capability and understanding of information systems remains a significant constraint in Indonesian public institutions. Therefore, the development of auditor digital capacity must be a priority in the national audit reform strategy. Conceptually, digital internal audit contributes directly to fraud prevention by enhancing risk prediction capabilities and strengthening process transparency. When internal audit can operate automatically, data-based, and in real-time, potential deviations can be identified earlier before escalating into major losses for the state. Thus, the implementation of digital internal audit is not just a technological innovation but an integral part of the national strategy to strengthen the accountability and integrity of public finance in the digital era.

3. Methods

The Systematic Literature Review (SLR) approach is utilized in this study to identify, assess, and synthesize various empirical findings related to the relationship between digital transformation, internal control systems, internal audit, and fraud prevention in the public sector. This process was conducted through four main

stages: (1) source identification, (2) literature selection, (3) data extraction, and (4) thematic analysis. The first stage, source identification, was performed by searching academic publications from Google Scholar, Research Gate and national journal databases indexed. The publication year range was limited to the five years period to ensure current relevance to the developments in audit digitalization and public financial governance.

The initial search yielded over some articles discussing internal control, internal audit, and fraud prevention. However, after the screening process with inclusion criteria (relevant topic, clear methodology, and focus on the public sector or financial institutions), several selected articles were retained as the basis for analysis. The second stage, literature selection, considered the originality of the data and the context of implementation in Indonesia. Investigate the effectiveness of technology-based control systems in improving the efficiency of financial anomaly detection.

The third stage, data extraction, involved identifying the main variables that appeared repeatedly in the literature: (a) the level of digital transformation implementation, (b) the adaptability of the internal control system, (c) the competence of digital auditors, and (d) the effectiveness of fraud prevention. These variables formed the basis for analyzing the relationships between concepts within the public financial context. The fourth stage, thematic analysis, found that the majority of studies affirm the importance of integrating digital technology and strengthening auditor capacity. This combination has been proven to enhance the accuracy of financial oversight and minimize opportunities for deviation.

Furthermore, the SLR results indicate that the implementation of continuous auditing and data-driven control systems is the new direction in managing digital fraud risk in government agencies.

4. Results

The results of the literature analysis indicate that digital transformation has brought about fundamental changes to the mechanisms of financial management in the public sector, both in terms of efficiency and the resulting risks. The digitalization of accounting, audit, and internal control processes drives the government to update working systems from manual to automated and integrated ones. This digitalization process accelerates the flow of financial information and enables faster and more transparent reporting. However, beneath this progress, new challenges arise in the form of cyber security risks, data misuse, and the increased complexity of fraud that exploits technology loopholes.

Key findings from various studies confirm that traditional internal control systems based on manual procedures are no longer adequate to anticipate digital-based threats. Nurdin et al. (2019) mention that internal control systems need to be adaptively updated to be able to respond to the risk dynamics arising from digital transformation. The application of e-control and data-driven monitoring is proven to enhance an organization's capability in early detection of financial transaction irregularities. Such systems use automated algorithms to identify anomalies in accounting data, thereby reducing the space for financial report manipulation.

The literature results also affirm that the integration of digital technology in internal audit expands oversight capacity and accelerates the fraud detection process. Prasetyo (2023) found that auditors using digital audit tools are capable of identifying transactional errors up faster compared to manual methods. Technology-based audit not only improves time efficiency but also expands the scope of examination, including the analysis of non-financial data such as electronic traces and system activity logs. This approach allows auditors to assess the reliability of financial processes holistically and objectively. Besides improving efficiency, digitalization also strengthens public transparency through the broad availability of accessible financial data. The implementation of online-based financial systems enables continuous oversight across agencies and reduces the potential for moral hazard by limiting opportunities for manipulation and undisclosed transactions. Research by Bora et al. (2021) found that the adoption of internal control technology supported by real-time reporting significantly enhances public trust in local government accountability.

Real-time reporting allows financial information to be monitored continuously, creating a more open and responsive oversight environment. This digital system also accelerates the reporting process and supports faster fiscal decision-making because financial data can be reviewed and analyzed at any moment. Moreover, digital platforms provide structured, traceable, and timely information, which improves the overall quality of financial management. As a result, digitalization contributes not only to operational improvements but also to stronger

governance practices, better transparency standards, and increased public confidence in the integrity of government financial processes.

Despite the significant benefits of digitalization, several studies also highlight challenges in its implementation. Maharani (2023) assert that the effectiveness of adaptive control systems highly depends on the readiness of human resources, technological infrastructure, and organizational culture. Many public agencies still face a digital competency gap among auditors and financial staff. When the technological capability of auditors is inadequate, the implementation of digital systems can actually pose new risks, such as data input errors, information leaks, or even excessive reliance on software without manual validation.

The aspect of auditor competence is a major highlight in various studies. Rosli et al. (2020) conclude that digital literacy and the ability to use modern audit technology significantly influence the auditor's capability to detect and prevent fraud. Auditors who can integrate data analysis, system logs, and predictive modeling tend to be more effective in identifying suspicious transaction patterns. However, research also emphasizes the importance of the auditor's personal integrity as an equally critical factor compared to technical proficiency. Good internal control does not only rely on systems and technology but also on the ethical commitment of the individuals managing it.

The synthesis results also show that digital internal audit has a positive correlation with the effectiveness of fraud prevention in the public sector. A study by Wibowo (2023) in Islamic financial institutions indicates that the combination of digital audit and adaptive internal control can suppress deviation risk by up to 30%.

This finding is relevant to the government context because the risk patterns and control mechanisms are relatively similar: both require a balance between technology, governance, and auditor competence. Furthermore, the application of audit based on continuous monitoring is proven to accelerate the process of reporting non-compliance and encouraging corrective actions in real time.

Aside from the operational perspective, the literature also highlights policy and governance dimensions. Ginanjar and Syamsul (2020) assert that digital-based financial oversight policies need to be designed systematically, considering data security, procedural transparency, and regulatory compliance. Mismatches between policy and practice in the field often lead to the weak effectiveness of digital audit. Therefore, digital transformation must be accompanied by regulatory updates and risk-based oversight so that the implemented systems can run consistently and efficiently.

Another interesting finding relates to organizational culture and readiness for change. Maharani (2023) identified that resistance to technological change is the main inhibitory factor in the success of digital audit. In many public agencies, there is still a conservative paradigm that views digital audit only as a supplementary tool, not as the main foundation of modern oversight. This shift in mindset requires support from intensive training, effective organizational communication, and visionary leadership. Leadership that supports innovation will encourage faster acceptance of new technology and strengthen the synergy between auditors, management, and control systems.

Furthermore, the results of the literature analysis indicate that cross-agency collaboration and the use of big data represent emerging directions in public financial oversight. When government financial data is integrated across multiple agencies, the potential for redundancy, inconsistencies, and reporting errors can be significantly reduced. Cross-sector data integration also enhances the ability to identify early fraud indicators by enabling broader, real-time visibility across entities and financial activities. In addition, the application of big data analytics supports more accurate risk profiling, anomaly detection, and predictive assessments that strengthen fraud prevention efforts. However, this level of integration requires a robust cybersecurity framework and comprehensive data governance to ensure the confidentiality, integrity, and availability of information. Strong protection mechanisms are essential to safeguard sensitive financial data from cyber threats and unauthorized access.

Effective data governance is also needed to establish clear protocols, accountability structures, and quality standards in managing shared information systems across the public sector. Overall, the SLR results show that the effectiveness of internal control and digital audit in preventing fraud depends on three main elements. First, the readiness of technology and digital infrastructure that supports the implementation of automated oversight systems. Second, the competence and integrity of auditors who understand the technical aspects and professional ethics in data-based auditing. Third, the government's policy support for audit innovation and technology-based oversight. These three elements complement each other and form a resilient oversight framework against digital risks.

5. Discussion

The results of the literature review reveal that digitalization in public financial management not only changes operational systems but also the paradigm of oversight and accountability of state finances. Digital transformation demands that government institutions adapt structurally and functionally. This shift requires close collaboration between technology, policy, and human resources. Thus, the effectiveness of internal control is no longer measured solely by administrative compliance but also by the system's ability to detect, prevent, and respond to digital risks adaptively (Suhardjo et al., 2023).

The integration of digital audit is proven to be a strategic component in building transparent financial governance. The use of computer-assisted audit tools (CAATs), data analytics, and continuous monitoring systems expands the auditor's oversight capacity in tracing complex electronic transaction trails. Digital audit technology allows examinations to take place in real-time, so deviations can be identified faster than in conventional systems. However, the research also highlights that the adoption of audit technology without enhancing human competence only leads to procedural changes, not substantial transformation. Auditors who do not understand data analysis and cybersecurity may misinterpret digital audit results or ignore critical risk signals (Rosli et al., 2020).

From the perspective of the internal control system, the research findings of Maharani (2023) affirm that the effectiveness of adaptive systems is determined by the extent to which the organization can adjust its control structure to technological risks. When public organizations are capable of integrating data-based automated

control and cybersecurity policies, the level of fraud detection increases significantly. Conversely, if control focuses only on manual procedures without a digital response mechanism, the system becomes vulnerable to manipulation. This indicates that good digital governance is not only oriented towards the use of technology but also towards the integration of policies, infrastructure, and organizational behavior.

The aspect of organizational culture also influences the success of digital audit implementation. Many public agencies still face resistance to change, especially from employees accustomed to manual systems. The findings of Peng et al. (2021) show that this resistance can be minimized through transformational leadership and continuous training. When top management demonstrates a commitment to innovation, the level of acceptance of digital systems increases, and oversight effectiveness improves. In addition to internal factors, cross-agency collaboration and national data integration are important elements in strengthening digital fraud prevention. Bora et al. (2021) emphasize that cross-system oversight between agencies allows for early detection of suspicious transactions, particularly in the management of public funds involving various entities.

The big data approach expands the audit scope and enables correlative analysis across government work units. Conceptually, the results of this study support the view that digital transformation is not merely a technical issue but also a change in bureaucratic values and behavior. Digital audit, adaptive internal control, and auditor competence form an interconnected ecosystem in preventing fraud. All three are only effective if supported by ethical governance, integrative policies, and adequate technological readiness. By strengthening these three aspects, the

Indonesian public sector can create a financial oversight system that is more transparent, efficient, and resilient against digital fraud risks.

6. Conclusion

Digital transformation in government financial management has a dual impact: on one hand, it increases efficiency, transparency, and accountability, but on the other hand, it introduces new risks in the form of increasingly complex digital fraud. Based on a systematic review of the literature from last five years, it is concluded that the effectiveness of fraud prevention in the digital era relies on three main factors: the quality of the adaptive internal control system, the capability of digital auditors, and responsive institutional policy support for technological developments. Internal control systems that leverage information technology are proven to enhance the capacity for early detection of suspicious transactions and strengthen data-based oversight mechanisms.

Furthermore, the auditor's mastery of technology is a crucial element for the optimal utilization of digital systems. Strengthening human resource capacity through continuous training and the implementation of data-based auditing are strategic steps in reinforcing the integrity of state finances. Therefore, the oversight strategy in the public sector must be oriented towards integrated, adaptive, and ethically grounded digital governance. The government needs to ensure that technological innovation proceeds in parallel with the strengthening of competence and adequate control policies, in order to realize a public financial system that is transparent, resilient, and free from the risks of digital fraud.

References

- Bora, I., Duan, H. K., Vasarhelyi, M. A., Zhang, C., & Dai, J. (2021). The transformation of government accountability and reporting. *Journal of Emerging Technologies in Accounting*, 18(2), 1-21.
- Ginanjar, Y., & Syamsul, E. M. (2020). Peran auditor internal dalam pendeteksian dan pencegahan fraud pada bank syariah di kota bandung. *Jurnal Ilmiah Ekonomi Islam*, 6(3), 529-534.
- Maharani, R. (2023). Organizational Readiness for AI Adoption in Indonesian Manufacturing SMEs. *Journal of Sustainability Industrial Engineering and Management System*, 2(1), 120-129.
- Nurdin, Y., 'Tahar, F., & Nurbayani, N. (2019). Pengaruh Sistem Pengendalian Internal Terhadap Pencapaian Good Government Governance Melalui Pencegahan dan Pengungkapan Fraud. *Jurnal Akuntansi dan Pajak*, 19(02), 116-133.
- Peng, J., Li, M., Wang, Z., & Lin, Y. (2021). Transformational leadership and employees' reactions to organizational change: Evidence from a meta-analysis. *The Journal of applied behavioral science*, 57(3), 369-397.
- Prasetyo, D. E., Wulandari, G. A. A., & Meini, Z. (2023). Identifikasi Fraud Dalam Pemeriksaan Internal Melalui Data Analytics. *EQUITY*, 26(1).
- Putri, T. E., Kuntadi, C., & Pramukty, R. (2023). Faktor-faktor yang memengaruhi pencegahan kecurangan: Peran audit internal, sistem pengendalian internal dan komitmen organisasi. *Jurnal Economina*, 2(7), 1789-1802.

- Rashid, C. A. (2022). The role of internal control in fraud prevention and detection. *Journal of Global Economics and Business*, 3(8), 43-55.
- Rosli, R., Mohamed, I. S., Mohamed, N., Othman, R., & Rozzani, N. (2020). Development of fraud prevention (FP) model using the theory of planned behavior. *Business and Economic Research*, 10(3), 311.
- Suhardjo, S., Suharti, S., Suyono, S., Mukhsin, M., & Hadi, S. (2023, November). Digital Internal Controls: Safeguarding Data Integrity and Compliance in a Technologically Evolving Landscape. In *International Conference on Business Management and Accounting* (Vol. 2, No. 1, pp. 306-311).
- Wibowo, D. (2023). Pencegahan Fraud Melalui Audit Internal dan Pengendalian Internal pada Bank Syariah Indonesia. *Jurnal Ilmiah Ekonomi Islam*, 9(1), 1485-1491.