E-ISSN: 3123-2507
DOI: https://doi.org/10.64803/cessmuds.v1.113

The Role of Information Systems Audit in Preventing Data Processing Errors

Pasya Namira[1], Fayakhun Wibisono[2], Aisyah Nurhaliza Arifin[3] , Neng Sri Wardhani[4]

[1,2,3,4]Department of Accounting, Universitas Pembangunan Panca Budi, Medan, Indonesia
E-mail: [1]ravaabiaksa3@gmail.com , [2]Fayakhun97@gmail.com, [3]aisyahnurhaliza7@gmail.com,
[4*]nengsri_wardhani@dosen.pancabudi.ac.id
[*]E-mail Corresponding Author: ravaabiaksa3@gmail.com

Abstract

Information systems are essential components in modern organizations, supporting operational activities, financial reporting, and strategic decision-making. However, weaknesses in system controls may lead to data processing errors that reduce data accuracy, reliability, and integrity. This study aims to comprehensively analyze the role of information systems audit in preventing data processing errors through the evaluation of internal controls, audit procedures, and information technology governance frameworks. This research employs a qualitative approach using a systematic literature review of international journals and conference proceedings published between 2015 and 2025. The results show that information systems audits play a critical preventive role by identifying risks at the input, processing, and output stages, as well as by strengthening internal control effectiveness. The implementation of continuous and risk-based information systems audits enhances data quality, minimizes processing errors, and supports effective IT governance. This study contributes theoretically and practically by presenting a structured audit framework that can be applied to improve data processing accuracy and organizational performance.

Keyword: s*information systems audit; data processing errors; internal control; IT governance*

I. INTRODUCTION

The rapid advancement of information technology has transformed organizational data processing practices. Organizations increasingly depend on information systems to process large volumes of data efficiently and accurately. Despite these advantages, inadequate system controls expose organizations to data processing errors that may lead to inaccurate information, poor decision-making, and reduced stakeholder trust (Romney & Steinbart, 2021; Wilkin & Chenhall, 2010).

Data processing errors can occur at multiple stages, including data input, processing, storage, and output. Errors at the input stage often arise from unauthorized access or incorrect data entry, while processing errors may result from flawed system logic or unauthorized system changes. Output errors commonly involve incomplete or inaccurate reports. These risks highlight the importance of implementing effective control mechanisms within information systems (Li et al., 2012; Hunton et al., 2004).

Previous studies emphasize that information systems audit is a vital tool for evaluating the effectiveness of internal controls and IT governance. Frameworks such as COBIT 2019, ISO/IEC 27001, and COSO Internal Control provide structured guidance for managing IT risks and ensuring data integrity. However, many organizations still treat audits as post-event detection mechanisms rather than preventive instruments (De Haes et al., 2013; ISACA, 2019; ISO/IEC 27001, 2013).

This research addresses this gap by examining the preventive role of information systems audit in minimizing data processing errors. The objective of this study is to analyze how audit activities contribute to strengthening internal controls across all data processing stages and to propose a structured conceptual framework for error prevention (Tuttle & Vandervelde, 2007; Moeller, 2016).

In recent years, the complexity of organizational information systems has increased significantly due to the adoption of enterprise resource planning (ERP) systems, cloud computing, and integrated digital platforms. These technologies enable real-time data processing and cross-functional integration, but they also expand the risk surface for data processing errors. As system architectures become more complex, traditional manual controls are no longer sufficient to ensure data accuracy and integrity (Hunton et al., 2004; Sutton et al., 2016).

Furthermore, the growing reliance on data-driven decision-making places greater pressure on organizations to ensure the reliability of processed information. Inaccurate or delayed information may not only affect operational efficiency but also compromise strategic decisions and regulatory

compliance. Consequently, organizations require robust assurance mechanisms capable of identifying weaknesses in system controls before errors materialize (Wilkin & Chenhall, 2010; Moeller, 2016).

In this context, information systems audit is expected to evolve beyond periodic compliance assessments toward a more proactive and continuous assurance function. By systematically evaluating general controls, application controls, and IT governance structures, information systems audits can play a preventive role in reducing data processing errors. This perspective reinforces the relevance of the present study and highlights the need for a comprehensive framework that positions information systems audit as a critical component of error prevention in modern organizations (De Haes et al., 2013; ISACA, 2019).

II. RESEARCH METHODOLOGY

This study adopts a qualitative research design employing a systematic literature review (SLR) method to comprehensively examine the role of information systems audit in preventing data processing errors. The SLR approach is considered appropriate for synthesizing theoretical and empirical findings related to IT governance, internal control, and audit effectiveness across diverse organizational contexts (Alqahtani & Mayes, 2018; Wilkin & Chenhall, 2010).

Relevant literature was collected from reputable international academic databases, including Google Scholar, IEEE Xplore, ScienceDirect, and SpringerLink, which are widely used in prior information systems and accounting research (Romney & Steinbart, 2021; Sutton et al., 2016). The literature selection criteria included English-language publications, relevance to information systems audit and data processing accuracy, and studies published within the last ten years to ensure the currency and relevance of the findings (ISACA, 2019).

The research process consisted of four main stages: problem identification, literature collection, content analysis, and synthesis of findings. This structured process follows established guidelines for systematic reviews in information systems and IT governance research, enabling a transparent and replicable methodology (De Haes et al., 2013; Moeller, 2016).

Content analysis was conducted to identify recurring themes related to audit objectives, internal control mechanisms, risk mitigation, and preventive strategies in information systems environments. Prior studies emphasize that systematic content analysis is effective in uncovering patterns related to IT control weaknesses and audit responses across multiple organizational settings (Li et al., 2012; Tuttle & Vandervelde, 2007).

Based on the synthesis of the reviewed literature, a conceptual framework was developed to illustrate the relationship between information systems audit activities, internal control effectiveness, and data processing accuracy. This framework draws on IT governance principles and control models such as COBIT and ISO/IEC 27001, which highlight the alignment between audit functions, control maturity, and information reliability (ISACA, 2019; International Organization for Standardization, 2013).

To enhance the rigor of the systematic literature review, explicit inclusion and exclusion criteria were applied during the screening process. Inclusion criteria required that studies explicitly address information systems audit, internal control, IT governance, or data processing accuracy within organizational contexts. Studies lacking methodological clarity or not directly aligned with the research objectives were excluded, consistent with prior SLR practices in IT governance research (Alqahtani & Mayes, 2018; Wilkin & Chenhall, 2010).

The selected literature was analyzed using a qualitative coding approach. Each article was systematically reviewed and coded according to predefined categories, including audit scope, type of control evaluated (general controls or application controls), identified risks, and preventive outcomes. This approach is commonly used in audit and accounting information systems research to enable consistent comparison and synthesis across studies (Hunton et al., 2004; Romney & Steinbart, 2021).

To reduce selection bias and enhance validity, triangulation was applied by comparing findings across multiple databases, research designs, and organizational contexts. The synthesis process focused on integrating theoretical perspectives and empirical evidence to develop a coherent understanding of how information systems audit contributes to data processing error prevention. Although this study does not involve primary data collection, the structured and transparent review process supports the reliability and replicability of the

research methodology (De Haes et al., 2013; Moeller, 2016).

III. RESULTS AND DISCUSSION

This section presents the research results derived from the literature analysis and discusses them in relation to internal control theory and IT governance principles.

Table 1 summarizes the role of information systems audit in preventing data processing errors across the input, processing, and output stages.

Table 1. Mapping of Information Systems Audit Activities and Data Processing Error Prevention

Data Processing Stage	Potential Errors	Audit Focus	Preventive Controls
Input	Inaccurate data entry, unauthorized access	Authorization and validation	Input validation rules, role-based access control
Processing	Incorrect calculations, unauthorized system changes	Processing logic and change management	Automated controls, formal system testing

The findings indicate that at the input stage, information systems audits reduce errors by ensuring proper authorization and data validation mechanisms (Romney & Steinbart, 2021; Li et al., 2012). At the processing stage, audits ensure that system changes are formally approved, adequately tested, and properly documented, thereby minimizing processing-related risks and control weaknesses (Hunton et al., 2004; ISACA, 2019). At the output stage, information systems audits enhance the accuracy and reliability of reports through reconciliation procedures and exception reporting mechanisms (Tuttle & Vandervelde, 2007; International Organization for Standardization, 2013).

Table 2 provides a broader perspective by linking commonly used audit frameworks with types

of data processing errors and their organizational impact.

Table 2. Relationship Between Audit Frameworks, Data Processing Errors, and Organizational Impact

Audit Framework	Focus Area	Type of Error Prevented	Organizational Impact
COBIT 2019	IT governance and control objectives	Processing and control failures	Improved IT governance and regulatory compliance
ISO/IEC 27001	Information security management	Data integrity and security errors	Enhanced data protection and stakeholder trust
COSO Internal Control	Control environment and risk assessment	Input and reporting errors	Reliable financial and operational reporting
Continuous Auditing	Real-time monitoring and analytics	Transactional and system errors	Early detection and prevention of errors

The discussion confirms that information systems audit functions as a preventive mechanism rather than merely a detection tool. These findings are consistent with prior studies that emphasize the importance of continuous auditing and risk-based audit approaches in strengthening internalcontrolsand

improving data quality (De Haes et al., 2013; Moeller, 2016; ISACA, 2019).

A. CONCEPTUAL FRAMEWORK

Based on the research findings, the proposed conceptual framework explains the preventive role of information systems audit by illustrating a causal relationship between audit activities, internal control effectiveness, and data processing quality. Information systems audit activities—such as risk assessment, control evaluation, compliance testing, and continuous auditing—contribute to strengthening internal controls, including access controls, processing controls, and output controls. Enhanced

internal control effectiveness subsequently improves data processing quality in terms of accuracy, completeness, timeliness, and reliability. As a result, effective audit implementation reduces data processing errors and supports higher-quality organizational decision-making (ISACA, 2019; Romney & Steinbart, 2021; International Organization for Standardization, 2013).

IV. CONCLUSION

` This study concludes that information systems audits play a strategic and comprehensive role in preventing data processing errors by functioning not only as a detection mechanism but also as a preventive and continuous assurance process. Through systematic evaluation of controls at the input, processing, and output stages, information systems audits enhance data accuracy, system integrity, and overall information reliability, which are critical for effective managerial decision-making and organizational performance (Romney & Steinbart, 2021; Li et al., 2012).

The findings further indicate that preventive and continuous audit approaches, when supported by established governance and control frameworks such as COBIT 2019, ISO/IEC 27001, and the COSO internal control framework, significantly contribute to strengthening IT governance and internal control maturity. These frameworks provide structured guidance for risk assessment, control implementation, and compliance monitoring, thereby reducing the likelihood of data processing errors and control weaknesses in complex information systems environments (ISACA, 2019; International Organization for Standardization, 2013; De Haes et al., 2013).

Although this study is limited to a literature-based approach and does not involve primary empirical data, it offers a robust theoretical foundation and practical insights for organizations seeking to improve data processing quality through information systems audits. The structured synthesis of prior research enhances understanding of best practices in audit implementation and highlights the importance of aligning audit activities with organizational risk profiles and governance objectives. Future research is encouraged to empirically test the proposed relationships across different industries and organizational contexts to further validate and extend the findings of this study (Moeller, 2016; Wilkin & Chenhall, 2010).

V. RECOMMENDATIONS

A. Recommendations for Organizations and Practitioners

Organizations are strongly encouraged to implement information systems audits on a continuous and risk-based basis rather than relying solely on periodic audits. Continuous auditing supported by automated tools and data analytics can enhance the early detection and prevention of data processing errors across all stages of the data lifecycle. Management should ensure that both general controls (such as access control, change management, and system security) and application controls (such as input validation, processing controls, and output reconciliation) are properly designed and effectively implemented.

Furthermore, audit findings should be formally integrated into the system development life cycle (SDLC). By embedding audit recommendations during system design, development, and implementation phases, organizations can reduce the likelihood of recurring data processing errors. Training programs should also be provided to system users and IT personnel to increase awareness of data accuracy, control procedures, and audit compliance.

B. Recommendations for Regulators and Professional Bodies

Regulators and professional organizations are advised to promote the adoption of internationally recognized IT governance and audit frameworks, including COBIT 2019, ISO/IEC 27001, and the COSO Internal Control Framework. These frameworks provide structured guidance for managing IT risks and ensuring data integrity. Regulatory bodies may consider issuing more detailed technical guidelines and best practice recommendations to support organizations in implementing effective information systems audits.

In addition, professional bodies should enhance auditor competencies through continuous professional education programs focusing on emerging technologies, continuous auditing, and data analytics. Strengthening auditor skills will improve the effectiveness of audits in preventing data processing errors and supporting organizational governance.

C. Recommendations for Future Researchers

Future research is recommended to empirically test the conceptual framework proposed in this study. Researchers may employ quantitative methods, such as surveys or statistical modeling, to examine the relationship between information systems audit effectiveness and data processing accuracy. Qualitative approaches, including case studies and interviews, may also be used to gain deeper

insights into audit practices in different organizational contexts.

Additionally, future studies could explore the integration of advanced technologies, such as artificial intelligence, continuous auditing systems, and real-time monitoring tools, in enhancing the preventive role of information systems audits. Comparative studies across industries or organizational sizes would also contribute to a more comprehensive understanding of how audit practices influence data processing quality.

VI. REFERENCES

Alqahtani, F., & Mayes, K. (2018). Information security governance challenges and solutions: A systematic review. *Computers & Security, 76*, 227–244. https://doi.org/10.1016/j.cose.2018.03.002

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems, 27*(1), 307–324. https://doi.org/10.2308/isys-50422

Hunton, J. E., Wright, A. M., & Wright, S. (2004). Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? *Journal of Information Systems, 18*(2), 7–28. https://doi.org/10.2308/jis.2004.18.2.7

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. ISO. https://doi.org/10.3403/30297595

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.

Li, C., Peters, G. F., Richardson, V. J., & Watson, M. W. (2012). The consequences of information technology control weaknesses on management information systems: An empirical investigation. *Journal of Information Systems, 26*(2), 91–122. https://doi.org/10.2308/isys-50217

Moeller, R. R. (2016). *Executive's guide to IT governance: Improving systems processes with service management, COBIT, and ITIL* (2nd ed.). Wiley.

Romney, M. B., & Steinbart, P. J. (2021). *Accounting information systems* (15th ed.). Pearson Education.

Sutton, S. G., Holt, M., & Arnold, V. (2016). The reports of my death are greatly exaggerated—Artificial intelligence research in accounting. *International Journal of Accounting Information Systems, 22*, 60–73. https://doi.org/10.1016/j.accinf.2016.07.005Tuttle, B. M., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems, 8*(4), 240–263. https://doi.org/10.1016/j.accinf.2007.07.00

Wilkin, C. L., & Chenhall, R. H. (2010). A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems, 24*(2), 107–146. https://doi.org/10.2308/jis.2010.24.2.107

Yigitbasioglu, O. M., & Velcu, O. (2012). A review of dashboards in performance management: Implications for design and research. *International Journal of Accounting Information Systems, 13*(1), 41–59. https://doi.org/10.1016/j.accinf.2011.08.002