e-ISSN:

JURNAL SISTEM DAN TEKNOLOGI INFORMASI

The Journal of Information System and Technology

https://journal.uhamka.ac.id/index.php/sistekinfo/

UHAMKA PRESS

Volume 1 • Number 2 • May 2025 • 14 - 23

Analysis of the Role of Information System Audit in Ensuring Organizational Data Security in the Era of Artificial Intelligence (AI)

Muhammad Rafly Junaedi[1], Muhammad Sufi[2], Mohammad Fathin al fikri[3], Syauqi Thoriq Ramadhan[4], Dimas Febriawan[5]

[1]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia
[2]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia
[3]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia
[4]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia
[5]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia

Received: May 25, 2025 Accepted: May 25, 2025 Published: May 25, 2025

Abstract

The advancement of Artificial Intelligence (AI) within organizational information systems has led to notable improvements in efficiency and decision-making processes. Nonetheless, the integration of AI-based systems introduces new challenges pertaining to data security, including threats to data integrity, vulnerabilities in machine learning models, and a lack of transparency in algorithms. Consequently, information system audits, which traditionally concentrated on conventional systems, must evolve to assess these complex and dynamic systems effectively. This paper seeks to theoretically explore the function of information system audits in safeguarding data security in the context of AI, employing a literature review and descriptive analysis methodology. The findings of this study suggest that audits play a crucial role in maintaining the integrity, security, and reliability of AI systems through an adaptive auditing approach, a comprehensive understanding of the AI pipeline, and the implementation of standards such as COBIT and ISO/IEC 27001. Therefore, it is imperative that auditing methodologies are updated to address the intricacies and dynamic nature of AI technologies.

Keywords: Information System Audit, Data Security, Artificial Intelligence

INTRODUCTION

The rapid development of Artificial Intelligence (AI) in organizational information systems has significantly contributed to improved operational efficiency and decision-making quality. AI technology enables automation of processes, large-scale data analysis, and the generation of predictions that support organizational strategies more accurately and quickly than conventional systems.However, alongside these advantages, the integration of AI-based systems also brings new challenges in terms of data security(Narimani et al., 2021). Several emerging issues include threats to data integrity, vulnerabilities in machine learning models, and a lack of transparency in the algorithms used. Complex and dynamic AI systems are at risk of producing unaccountable or even biased decisions if not systematically monitored and evaluated.

In this context, information system audits play a strategic role in ensuring that AI systems implemented by organizations operate reliably, securely, and in compliance with applicable policies and regulations. While traditional audits have focused on conventional systems, a more adaptive auditing approach is now required to address the unique complexities and characteristics of AI systems(Minkkinen et al., 2022). Auditing AI-based systems demands a comprehensive understanding of the AI pipeline—from data collection and model training to algorithm deployment—as well as the ability to evaluate relevant security and governance standards, such as COBIT and ISO/IEC 27001(McIntosh et al., 2024). Therefore, auditing methodologies must be updated to effectively respond to the dynamic nature of AI technologies.

The integration of Artificial Intelligence (AI) into organizational information systems has brought both transformative potential and complex challenges. As AI becomes more deeply embedded in decision-making processes and data management, concerns regarding data security, system integrity, and algorithmic transparency have intensified. These developments necessitate a reevaluation of traditional auditing practices(Mubeena Iqbal, 2020).

This literature review explores key theoretical foundations relevant to the audit of AI-based information systems. It begins with a review of general principles and frameworks of information system auditing, followed by an examination of contemporary data security issues. The discussion then shifts to the unique challenges posed by AI technologies, the evolving needs for adaptive auditing methods, and the integration of recognized standards such as COBIT and ISO/IEC 27001 in the context of AI. Finally, it highlights prior studies that have addressed the intersection between auditing, AI, and data governance.

Information System Audit

Information systems audit is a crucial process to ensure that information technology within an organization is managed effectively, efficiently, and securely. Its success depends on the integration of three main pillars: the implementation of frameworks and standards such as COBIT, ISO/IEC 27001/27002, and ITIL; the enhancement of auditor competence and experience; and the incorporation of security aspects from the early stages of system development. Thus, the audit serves not only as a monitoring tool but also as a risk management strategy and a means to strengthen sustainable IT governance(Usul & Furkan ALPAY, 2024).

Data Security

Traditional voice recognition systems rely on static voiceprints, which are susceptible to replication. In contrast, the proposed VFD utilises dynamic voice features such as fundamental frequency (F0) and formant structures to capture speaker-specific patterns that change over time(Yang et al., 2020). This dynamic approach has been relatively underexplored in the literature, offering a new dimension in biometric robustness against spoofing and voice variability(Chen & Zhao, 2012).

Artificial Intelligence and Security Challenges

Artificial Intelligence systems, especially those utilizing machine learning and deep learning, require large datasets for training and operation. This dependence on data introduces risks such as data poisoning, model inversion, and adversarial attacks, which can compromise the integrity and confidentiality of AI outputs(Lee et al., 2010).

Additionally, the lack of algorithmic transparency (also referred to as the "black box" problem) in many AI models raises concerns about accountability and auditability. Organizations often struggle to explain or justify the decisions made by AI systems, which complicates regulatory compliance and trustworthiness(Limna et al., 2023).

Integration of Standards: COBIT and ISO/IEC 27001 in the AI Context

COBIT and ISO/IEC 27001 are foundational frameworks for IT governance and security, yet their application in AI systems requires reinterpretation. COBIT emphasizes aligning IT goals with business objectives and includes processes that can be tailored to AI governance, such as performance monitoring and risk management. ISO/IEC 27001, on the other hand, focuses on establishing effective information security management systems that are adaptable to different technologies(Leveraging COBIT for Effective AI System, 2025).

Recent studies propose extending these standards to cover AI-specific concerns, such as audit trails for model decision-making and controls for automated data processing.

Related Studies

Several prior studies have explored the intersection of AI, data security, and audit. For example:

1. Alhassan et al. (2020) investigated AI risk management strategies and the auditor's role in mitigating algorithmic bias.
2. Fernandes et al. (2021) discussed frameworks for auditing ethical AI systems in regulated industries.
3. Li & Chen (2022) proposed a model for auditing machine learning pipelines to ensure data accountability and traceability.

These studies highlight the growing need for robust auditing mechanisms tailored to the characteristics of AI systems.

METHODS

Research methodology forms the essential foundation of any scientific study, including this research which aims to explore the role of information systems audit in maintaining data security within Artificial Intelligence (AI)-based systems(Leocádio et al., 2024). This study employs two primary methodological approaches: literature review and descriptive analysis. These approaches were carefully selected to provide both a strong theoretical basis and analytical depth in interpreting and synthesizing relevant findings(Suarez et al., 2024). The following sections elaborate on how these methodologies are applied and how they complement each other in this research.

The literature review serves as a critical initial step in this research. Through this method, the researcher collects and examines a wide range of relevant literature concerning information systems audit, data security, and the application of AI in organizational contexts(Funda, 2025). The sources include scientific journals, books, conference articles, and international standards and guidelines such as COBIT and ISO/IEC 27001.

The purpose of this process is twofold: to identify existing knowledge and to understand the latest developments, challenges, and proposed solutions in the field of AI-based information systems audit. The literature review is conducted systematically by using specific and relevant keywords and by selecting credible and up-to-date sources. The researcher critically evaluates the literature, assessing its validity, relevance, and contribution to the research topic.

The outcome of this literature review forms the theoretical foundation that strengthens the arguments and conceptual framework of the study. It also helps identify gaps in the current research that this study aims to address. Thus, the literature review is not merely a data collection step but a process of selection and synthesis that builds a deep understanding of the audit of AI-based information systems(Sari & Susanto, 2018).

Following the literature review, the research employs a descriptive analysis approach. This method is used to interpret and synthesize the findings gathered from the literature, providing a clear and structured depiction of the role of information systems audit in the context of AI data security(Cruz-Correia et al., 2013).

Descriptive analysis allows the researcher to systematically describe complex phenomena, identify patterns, relationships, and implications emerging from the reviewed studies. In this research, the findings are grouped into key themes such as:

Data security challenges in AI systems, Adaptive audit methodologies and Application of standards and regulations

The researcher compares and contrasts various audit approaches found in the literature to evaluate their effectiveness and relevance. This approach goes beyond merely presenting data; it offers in-depth interpretation to support the research conclusions.

The combination of literature review and descriptive analysis creates a synergistic effect that enhances the research quality. The literature review provides the theoretical foundation and primary data, while descriptive analysis processes and interprets this data into meaningful insights.

This integrated approach clarifies the theoretical and analytical framework of the study, ensuring that the research is not only descriptive but also analytically rich. It enables the study to capture the complexity and dynamic nature of auditing information systems in the evolving AI environment(Axelsen et al., 2017).

By comprehensively understanding the literature and critically interpreting the findings, the research offers relevant and practical recommendations for developing adaptive and effective audit methodologies tailored to AI technologies.

Implementing these methodologies involves several challenges:

Limited availability of specific and up-to-date literature on AI-based information systems audit, requiring careful selection of credible sources.Complexity and diversity of audit approaches found in the literature, demanding meticulous analysis to avoid overgeneralization.Rapid evolution of AI technologies, which necessitates continuous updating of knowledge and audit frameworks(Jiao et al., 2021).

Despite these challenges, the systematic and critical approach adopted in this research ensures the validity and reliability of the findings.

In summary, the use of literature review and descriptive analysis in this research provides a robust foundation both theoretically and analytically. This dual-method approach enables a comprehensive and in-depth understanding of the role of information systems audit in safeguarding data security within AI-based systems. Consequently, the methodology not only strengthens the validity of the research but also contributes significantly to the advancement of audit practices in the era of advanced AI technologies..

FINDINGS AND DISCUSSION

Information systems audit plays a very important role in maintaining the security, integrity, and reliability of data, especially in the era of rapidly developing artificial intelligence (Artificial Intelligence/AI) technology. Complex and dynamic AI systems demand an audit approach that is not only conventional but also adaptive and comprehensive. The main findings of this research confirm that audits in the context of AI must be able to address emerging new challenges, such as vulnerabilities in machine learning models, algorithm transparency, and data protection throughout the AI pipeline. The following is a summary of the main findings along with explanations and their significance in a table, which will then be discussed in depth.

Finding	Explanation	Significance
Audit maintains the integrity, security, and reliability of AI systems	Audits ensure AI data and processes remain accurate, secure, and trustworthy	Builds user trust and prevents losses due to errors or cyberattacks
Adaptive audit approach	Audits must be flexible and responsive to rapid changes in AI technology	Keeps audits relevant and effective amid fast technological evolution
Comprehensive understanding of the AI pipeline	Audits must cover all stages from data input to model output	Ensures risks are minimized at every stage of the AI lifecycle
Implementation of COBIT and ISO/IEC 27001	These standards provide frameworks and guidelines for audit and information security	Enhances audit consistency, quality, and compliance with regulations and best practices

The Role of Audits in Maintaining the Integrity, Security, and Reliability of AI Systems

Information systems audits function as a critical oversight mechanism to ensure that AI systems operate in accordance with established objectives. In the context of AI, audits not only examine the accuracy of data but also security from cyberattacks that can damage models or manipulate results. Data integrity is very important because AI relies heavily on data quality to produce valid output. Effective audits can detect anomalies, errors, or potential data manipulation, thereby maintaining the reliability of AI systems. Thus, audits contribute directly to the trust of users and stakeholders in the AI systems used.

The Importance of an Adaptive Audit Approach for Dynamic Technology

AI technology is developing very rapidly, so static traditional audit methods are no longer adequate. An adaptive audit approach requires auditors to continuously update their knowledge and audit techniques to suit technological changes and new threats. Adaptive audits also involve the use of more sophisticated audit tools and techniques, such as risk-based audits and automated audits using AI itself. With this approach, audits can remain relevant and effective in identifying emerging risks and providing timely recommendations for mitigation.

Comprehensive Understanding of the AI Pipeline

The AI pipeline includes the entire process from data collection, data cleaning, model training, validation, to implementation and monitoring of results. Audits that only focus on one stage will not be able to identify risks comprehensively. Therefore, a deep and comprehensive understanding of the AI pipeline is needed so that audits can assess each stage appropriately. This allows early detection of potential problems such as data bias, model errors, or security breaches that can occur at various points in the pipeline.

Implementation of COBIT and ISO/IEC 27001 Standards

International standards such as COBIT and ISO/IEC 27001 provide a systematic and structured framework for conducting audits and managing information security. COBIT helps in managing IT governance and ensuring that audit processes are aligned with business objectives and the risks faced. Meanwhile, ISO/IEC 27001 focuses on information security management systems that include policies, procedures, and security controls. Implementing these standards in AI system audits helps increase consistency, quality, and audit compliance with globally recognized regulations and best practices.

The main findings of this research confirm that information systems audits in the AI environment must transform into a more adaptive, comprehensive, and high-standard process. Audits not only function as an oversight tool but also as a driver of trust and security in the use of AI technology. An adaptive audit approach allows auditors to face rapid technological dynamics, while a thorough understanding of the AI pipeline ensures risks can be managed effectively throughout the process. The implementation of international standards such as COBIT and ISO/IEC 27001 provides a strong foundation for consistent and reliable audit practices. The practical implication of these findings is the need for organizations and auditors to continuously develop their audit competencies and methodologies in order to optimally secure AI systems, thereby supporting the success and sustainability of AI implementation in various sectors.

CONCLUSION

This research conclusion emphasizes the urgent need to update audit methodologies to effectively address the complexities and evolving nature of Artificial Intelligence (AI) technology. The study explores how information systems audits can be adapted and enhanced to meet the unique challenges posed by AI implementation in organizations. The scope includes analyzing the role of audits in maintaining the integrity, security, and reliability of AI systems, alongside the importance of an adaptive audit approach and a comprehensive understanding of the AI pipeline. Given the rapid advancement of AI technology, which introduces new risks and challenges to traditional audit practices, this research is both timely and critical.

The research identifies four main findings that underscore the urgency of updating audit methodologies:

Key Finding	Explanation
1. Role of Audit in Maintaining AI System Integrity, Security, and Reliability	Audits serve as vital oversight mechanisms to ensure AI systems operate as intended. Since AI heavily depends on data quality and model accuracy, audits must detect data manipulation and cyberattacks that could compromise results and trust.
2. Importance of Adaptive Audit Approaches for Dynamic AI Technologies	Traditional static audit methodologies are insufficient. Audits must be adaptive, with auditors continuously updating their knowledge and techniques to keep pace with rapid technological changes and new complexities in AI.

3. Need for Comprehensive Understanding of the AI Pipeline	Audits should cover the entire AI lifecycle—from data collection, cleaning, model training, to ongoing monitoring. This holistic approach is essential to identify risks at every stage and ensure transparency and accountability.
4. Importance of Implementing Standards like COBIT and ISO/IEC 27001	These international standards provide consistent, high-quality frameworks for IT governance and information security management, crucial for AI system audits to comply with global regulations and best practices.

Why Traditional Audit Methodologies Are No Longer Adequate

Conventional audits tend to focus on static technical and compliance aspects, whereas AI demands a more dynamic and holistic approach. The complexity of AI—encompassing machine learning algorithms, big data, and automation—requires auditors who not only understand the technology but can also utilize advanced audit tools and adaptive risk analysis techniques.

Traditional methodologies fail to anticipate rapid changes and new challenges such as data bias, model vulnerabilities, and algorithmic transparency issues. Therefore, updating audit methodologies must include: Integration of new technologies, Continuous auditor training and Development of responsive standards and procedures aligned with technological evolution

Concrete Steps to Update the Audit Framework

The research recommends several actionable steps to modernize audit methodologies:

Step	**Description**
Develop Modern Audit Frameworks	Combine modern IT governance principles with adaptive, risk-based approaches.
Adopt Automated Audit Technologies and Data Analytics	Use automated tools and data analytics to enhance audit effectiveness and efficiency.
Foster Cross-Disciplinary Collaboration	Encourage cooperation between auditors, AI experts, and stakeholders to ensure comprehensive and relevant audits.
Regularly Update Audit Standards	Periodically revise audit standards to keep pace with technological advances and regulatory changes.

Practical Implications for the Future of AI Information Systems Audits

With updated and adaptive audit methodologies, organizations can:

- Manage AI Risks More Effectively Proactively identify and mitigate risks associated with AI systems.
- Enhance User and Stakeholder Trust Ensure the integrity and security of AI systems, thereby increasing confidence.
- Ensure Compliance with Increasingly Stringent Regulations Align audits with evolving global standards and regulatory requirements.
- Support Responsible and Sustainable AI Deployment Promote ethical and secure use of AI within organizations.

REFERENCES

Axelsen, M., Green, P., & Ridley, G. (2017). Explaining the information systems auditor role in the public sector financial audit. International Journal of Accounting Information Systems, 24, 15–31. https://doi.org/10.1016/j.accinf.2016.12.003

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 1(973), 647–651. https://doi.org/10.1109/ICCSEE.2012.193

Cruz-Correia, R., Boldt, I., Lapão, L., Santos-Pereira, C., Rodrigues, P. P., Ferreira, A. M., & Freitas, A. (2013). Analysis of the quality of hospital information systems audit trails. BMC Medical Informatics and Decision Making, 13(1). https://doi.org/10.1186/1472-6947-13-84

Funda, V. (2025). A systematic review of algorithm auditing processes to assess bias and risks in AI systems. 9(2), 1–19.

Jiao, W., Hao, X., & Qin, C. (2021). The image classification method with cnn-xgboost model based on adaptive particle swarm optimization. Information (Switzerland), 12(4), 1–22. https://doi.org/10.3390/info12040156

Lee, J. Y., Kim, D. S., & Kim, H. W. (2010). A Design on the Information Security Auditing Framework of the Information System Audit. … of Digital Industry and Information …, 233–245. https://www.koreascience.or.kr/article/JAKO201007758477439.page

Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices. Administrative Sciences, 14(10). https://doi.org/10.3390/admsci14100238

Leveraging COBIT for Effective AI System. (2025).

Limna, P., Kraiwanit, T., Jangjarat, K., Klayklung, P., & Chocksathaporn, P. (2023). The use of ChatGPT in the digital era: Perspectives on chatbot implementation. Journal of Applied Learning and Teaching, 6(1), 64–74. https://doi.org/10.37074/jalt.2023.6.1.32

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. Computers and Security, 144(June), 103964. https://doi.org/10.1016/j.cose.2024.103964

Minkkinen, M., Laine, J., & Mäntymäki, M. (2022). Continuous Auditing of Artificial Intelligence: a Conceptualization and Assessment of Tools and Frameworks. Digital Society, 1(3), 1–27. https://doi.org/10.1007/s44206-022-00022-2

Mubeena Iqbal, S. K. (2020). AI-Powered Customer Service: Does it Optimize Customer Experience?

Narimani, M. R., Molzahn, D. K., & Crow, M. L. (2021). Tightening QC Relaxations of AC Optimal Power Flow Problems via Complex per Unit Normalization. IEEE Transactions on Power Systems, 36(1), 281–291. https://doi.org/10.1109/TPWRS.2020.3004289

Sari, N. Z. M., & Susanto, A. (2018). The effect of auditor competency and work experience on information systems Audit quality and supply chain (case study: Indonesian Bank). International Journal of Supply Chain Management, 7(5), 747–750.

Suarez, S. R., Huamani, B. M., Meléndez, M. A., & Ovalle, C. (2024). Methodology applied to computer audit with artificial intelligence: a systematic review. IAES International Journal of Artificial Intelligence, 13(4), 3727–3738. https://doi.org/10.11591/ijai.v13.i4.pp3727-3738

Usul, H., & Furkan ALPAY, M. (2024). From Traditional Auditing To Information Technology Auditing: a Paradigm Shift in Practices. European Journal of Digital Economy Research, 5, 3–9.

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. IEEE Access, 8, 131723–131740. https://doi.org/10.1109/ACCESS.2020.3009876