Global Economics and Finance Insights, Vol. 01, No. 1, PP 55-64, year 2026

RISK BASED INFORMATION SYSTEM AUDIT: A LITERATURE REVIEW AND ITS IMPLICATIONS IN ACCOUNTING

Mia Aristya Putri[1*]

[1] Indonesian School of Economics (STIESIA), Surabaya, Indonesia
[*]miaaristyaputri@gmail.com

ABSTRACT

This study analyzes the concept of Risk Based Information System Auditing (RBISA) and its relevance in the accounting profession. In line with the rapid growth of digital technology and the widespread use of automated accounting systems, organizations require more flexible and risk focused auditing approaches. Based on prior research and recognized frameworks such as COBIT, ITAF, and COSO, this paper evaluates how a risk based audit approach improves the effectiveness, accuracy, and trustworthiness of financial information systems. It explains the fundamental components of RBISA, including risk identification, risk evaluation, control examination, and audit reporting, and discusses its contribution to enhancing internal control systems, increasing audit productivity, and promoting proactive risk mitigation. Additionally, the study addresses the use of technological advancements such as data analytics and automated audit documentation, which enhance audit performance while simultaneously demanding higher technical competencies from auditors. The results indicate that implementing RBISA supports stronger corporate governance, greater financial accountability, and better compliance with regulatory requirements. Overall, this paper emphasizes the necessity of combining risk oriented and technology based auditing strategies in contemporary accounting practices to strengthen organizational accountability and long term resilience.

Keywords: risk based auditing, information technology, accounting systems, internal controls.

INTRODUCTION

In digital era, companies depend greatly on information technology (IT) to manage and process financial data. Because of this dependency, the reliability and security of IT systems become very important to support accurate managerial decisions and trustworthy financial reporting. An Information System (IS) Audit can be understood as a systematic evaluation of an organization's IT structure, operational activities, and control mechanisms to ensure that information assets are well protected, data accuracy is maintained, and systems operate effectively and efficiently (Moeller, 2011).

In modern accounting practices, IS audits play an essential role in safeguarding the confidentiality, integrity, and availability of financial information. They also help organizations comply with internal control frameworks and governance standards such as COSO and COBIT (ISACA, 2020). Over time, audit approaches have developed from traditional compliance based methods to more flexible and analytical risk based auditing (RBA) models. This shift shows that auditors now focus more on areas with the highest risk instead of testing all parts of

the system equally. In the context of information systems auditing, applying a risk based approach enables auditors to detect potential weaknesses that could affect the reliability of financial reporting, the effectiveness of IT governance, or overall organizational performance. By aligning audit activities with identified risk levels, this method increases audit efficiency, improves accuracy, and enhances the strategic contribution of the audit function, especially in complex technological environments.

Therefore, this paper aims to review previous studies related to risk based information system auditing and examine its importance in the accounting field. Specifically, this research analyzes how risk based auditing approaches can improve audit quality, strengthen internal control systems, and support better corporate governance in accounting systems that rely heavily on technology.

THEORETICAL BACKGROUND

Concept of Information System Audit

An Information System (IS) Audit is a systematic activity carried out to review and evaluate an organization's IT environment, including its controls, policies, and operational processes. The main purpose of this audit is to determine whether the information systems are capable of protecting company assets, maintaining data accuracy, and operating efficiently in line with organizational objectives. Based on the frameworks developed by ISACA, such as COBIT (Control Objectives for Information and Related Technologies) and ITAF (IS Audit and Assurance Framework), IS audits are designed to ensure that information assets comply with the three fundamental principles known as confidentiality, integrity, and availability (CIA). These principles are the core foundation of IT governance because they ensure that information remains secure, accurate, and accessible when needed. Through the evaluation of various control components such as user access controls, network security systems, backup and recovery procedures, and system change management IS audits provide assurance that IT systems function properly and securely. In addition, they confirm that these systems effectively support financial reporting activities in a reliable and protected manner.

Risk Based Audit Approach

The Risk Based Audit (RBA) approach is a contemporary audit concept that places risk identification and evaluation as the main basis of the auditing process. Different from traditional audits that focus mainly on compliance and apply the same testing procedures to all areas, RBA concentrates more on aspects that have the greatest potential risk in preventing the organization from achieving its goals. In this approach, auditors systematically identify

possible risks, analyze the probability and impact of those risks, and then design appropriate audit procedures to evaluate whether internal controls are effective in reducing them.

In the field of Information System Auditing, a risk based approach pays special attention to IT related threats such as unauthorized access to data, data alteration, system failures, and cyberattacks. These risks may affect the reliability and accuracy of financial as well as operational information. By focusing on high risk areas first, auditors can use audit resources more efficiently, improve assurance over internal controls, and enhance the overall quality of the audit. This approach is highly relevant in the current digital era, where organizations rely heavily on integrated information systems to process and store important financial data. Therefore, implementing risk based audit principles in IS audits supports proactive risk management and helps strengthen governance practices and accountability within organizations (Pathak, 2018; Knechel, 2007).

Integration with Accounting Systems

Today's accounting systems such as Enterprise Resource Planning (ERP), cloud based accounting platforms, and integrated financial management systems are highly dependent on advanced information technology infrastructure. These systems automatically record, process, and generate financial reports, which means that the quality of IT controls directly affects the accuracy and reliability of financial information. If there are weaknesses in IT controls, such as poor access control, lack of proper encryption, or limited system supervision, this can lead to errors, data manipulation, or even fraudulent activities.

Therefore, the implementation of Risk Based Information System Auditing (RBISA) in accounting processes becomes very important to ensure that financial audits are reliable and compliant with regulations. RBISA supports financial auditors by evaluating whether the systems that produce financial data are secure, effective, and trustworthy. This approach also helps organizations comply with internal control frameworks such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) and regulatory requirements like the Sarbanes Oxley Act (SOX), both of which stress the importance of strong internal control over financial reporting. In this context, IS audits act as a bridge between technological assurance and financial accuracy, ensuring that information used in decision making is secure and dependable from both operational and cybersecurity risks.

By applying risk based IS auditing principles within accounting systems, organizations are better able to identify irregularities, maintain data accuracy, and continuously improve both IT governance and financial oversight. This development reflects a significant shift in the accounting profession, where auditors are now required not only to understand accounting

standards but also to analyze and evaluate the technology systems that support financial reporting.

LITERATURE REVIEW

Risk Based Auditing: Concept and Effectiveness

Risk based auditing (RBA) is considered a more modern and strategic development in auditing practices because it prioritizes the evaluation of risks that could hinder an organization from achieving its goals. Unlike traditional compliance oriented audits that apply similar testing procedures to all areas, RBA concentrates on sections that have the highest level of risk, both in terms of likelihood and potential impact (Knechel, 2007). The main idea behind this approach is to allocate audit resources more effectively by focusing on high risk areas, so the audit process becomes more efficient and provides better assurance (Pathak, 2018).

By focusing on the most significant risk exposures, RBA encourages a proactive approach to risk management. It helps organizations identify and address possible threats before they develop into serious problems. This method also strengthens financial stability because it allows auditors to detect weaknesses in internal controls and operational processes at an early stage. Furthermore, RBA plays an important role in fraud prevention and detection, since auditors can design targeted procedures aimed at high risk activities and assess how strong the existing control systems are (O'Donnell & Schultz, 2005).

Research findings also show that RBA has a positive impact on financial performance and the quality of internal controls. Knechel et al. (2016) found that organizations implementing risk based audit strategies tend to achieve higher audit efficiency and improved assurance outcomes. Similarly, Al-Hatmi and Al-Hatmi (2021) concluded that the use of RBA enhances financial transparency and reduces audit costs by directing audit attention toward key risks that influence the reliability of financial reporting.

Importance of Technology in Information System Audit

The fast development of technology has significantly changed the practice of information system auditing. Various advanced tools, such as audit analytics, data mining techniques, and automated audit trails, are now widely used to improve audit quality and increase the reliability of financial information (Bierstaker et al., 2014). With the help of these technologies, auditors are able to process and analyze large volumes of data in real time, identify unusual transactions, and detect weaknesses in internal controls more effectively compared to traditional manual methods. In addition, the use of continuous auditing systems

allows auditors to monitor IT and financial controls on an ongoing basis, so they can provide faster feedback and recommend corrective actions when needed (Vasarhelyi et al., 2015).

The adoption of automation and digital tools also enhances audit consistency and reduces the risk of human error, as audit evidence can be documented systematically. As a result, the role of auditors has shifted from mainly collecting data to analyzing risk information and giving more strategic recommendations. This transformation ultimately leads to more effective and value added audit results. However, increased dependence on technology also creates new challenges. Modern IT systems are becoming more complex, which means auditors must possess broader competencies, including not only accounting expertise but also skills in data analytics, cybersecurity, and information system management (Kokina & Davenport, 2017). Moreover, because technology continues to evolve rapidly, auditors may face knowledge gaps if they do not continuously update their skills through professional training. The investment required to implement advanced audit technologies can also be expensive, which may become a limitation, especially for small and medium sized audit firms.

Implications for Accounting

The combination of risk based auditing and modern technology provides significant impacts on today's accounting practices. When audit quality improves and risks are managed more effectively, the reliability and credibility of financial reports also increase. This is very important to maintain investor trust and stakeholder confidence (Bierstaker et al., 2014). By making sure that financial information is produced, processed, and secured within a strong internal control system, organizations can enhance transparency and accountability.

In addition, the collaboration between risk based auditing (RBA) and technological tools strengthens corporate governance and supports better managerial decision making. Auditors who implement risk based methods supported by data analytics are able to provide insights that go beyond simply meeting regulatory requirements. For example, they can identify new or emerging risks, recommend improvements in internal controls, and align audit results with the organization's strategic objectives (Alles & Gray, 2020). Overall, this integration creates a more adaptive and future oriented accounting environment. The audit function is no longer limited to verifying financial accuracy, but also plays an important role in supporting long term organizational stability, sustainability, and value creation.

METHODS OF RESEARCH

Risk Based Information System Auditing (RBISA) is carried out through a structured approach that focuses audit activities on areas with the highest level of risk. Generally, this

method consists of four main stages: risk identification, risk assessment, control testing, and reporting with recommendations. Each of these stages is important to help auditors understand how different risks can affect the accuracy, reliability, and security of accounting information systems.

The first stage is risk identification, where auditors identify various IT related threats that could disrupt accounting processes or reduce the accuracy of financial data. These risks may arise from unauthorized access, data alteration, system errors, cyberattacks, or weaknesses within the system itself. By understanding the type and source of these risks, auditors can design a more focused audit plan that prioritizes the most critical risk areas (Pathak, 2018).

The second stage is risk assessment, which involves analyzing how likely each risk is to occur and how significant its impact could be on organizational goals and the reliability of financial reporting. Auditors usually use tools such as risk matrices or control self assessment methods to classify and rank risks based on their probability and potential impact (Knechel, 2007). A proper risk assessment helps ensure that audit resources are allocated efficiently, with greater attention given to high risk areas.

Next is the control testing stage. In this phase, auditors evaluate whether the internal controls implemented by the organization are effective in reducing the identified risks. This can include reviewing access control systems, password policies, backup procedures, and change management processes. Auditors use both qualitative evaluations and quantitative analysis to determine whether these controls are operating properly and providing adequate assurance over the reliability of accounting information (Moeller, 2011). Nowadays, many auditors also utilize automated audit analytics tools to examine large amounts of data, detect unusual patterns, and improve the accuracy and efficiency of their evaluations (Bierstaker et al., 2014).

The final stage is reporting and providing recommendations. At this point, auditors present their findings to management by explaining the identified risks, weaknesses in internal controls, and any compliance issues. They also offer practical suggestions to improve IT governance, strengthen control systems, and enhance overall risk management. This stage not only supports better managerial decision making but also encourages continuous improvement, as organizations are prompted to adjust their control systems in response to technological developments and emerging risks.

Overall, this risk based auditing approach combines systematic analysis with strategic thinking. It enables auditors to provide assurance that goes beyond simply meeting regulatory requirements. By integrating professional judgment with data driven techniques, RBISA

improves audit accuracy, supports proactive risk management, and strengthens the reliability and credibility of accounting information systems.

RESULT AND DISCUSSION

Implications for Accounting

The implementation of Risk Based Information System Auditing (RBISA) has created major changes in the accounting profession. It has transformed the way auditors and accountants evaluate internal controls, manage risks, and ensure the accuracy of financial reports, especially in a business environment that is highly dependent on technology. As companies increasingly rely on information systems to process and secure financial data, applying a risk based audit approach has become essential to maintain audit quality, operational effectiveness, and strong governance.

One of the main impacts of RBISA is its improvement in evaluating internal controls within accounting systems. Traditional audits usually focused on compliance and checking transactions in detail. In contrast, RBISA allows auditors to assess IT related controls that directly affect the reliability of financial information. These controls include user access restrictions, encryption systems, change management procedures, and data backup mechanisms that are designed to prevent unauthorized access, data manipulation, or data loss. Through a risk focused perspective, auditors can identify control weaknesses that might not be detected in conventional audits, which ultimately increases the reliability of accounting information. This approach is consistent with governance frameworks such as COSO and COBIT that emphasize the importance of risk management and effective internal controls (ISACA, 2020). RBISA also enhances audit efficiency and effectiveness. Instead of applying the same audit procedures to all areas, auditors concentrate on systems or processes that have the highest risk levels. This helps optimize audit resources and reduce unnecessary testing. As a result, audits can be completed more quickly and at lower cost, while still maintaining high quality. The use of audit analytics and automation tools further supports this efficiency, as auditors can analyze large volumes of data, detect unusual patterns, and monitor transactions in real time. This enables auditors to provide more meaningful insights and strategic recommendations to management (Pathak, 2018).

Another important effect of RBISA is the stronger connection between information system audits and financial audits. In today's digital accounting systems, IT processes are directly linked to financial reporting. Therefore, findings from IS audits such as issues related to data accuracy, system reliability, or access controls can significantly influence financial

audit assessments. For example, if weaknesses are found in an ERP system or automated journal entry process, financial auditors can consider these risks when evaluating the possibility of material misstatements (Moeller, 2011). This integration creates a more comprehensive assurance framework and reduces the risk of overlooking IT related problems that may affect financial reporting.

RBISA also contributes to stronger corporate governance and accountability. By aligning audit activities with the organization's overall risk management strategy, RBISA supports transparency, regulatory compliance, and effective risk oversight. It ensures that management is responsible for maintaining strong internal controls and responding to identified risks. This alignment increases stakeholder trust in financial reports and governance practices. Additionally, it encourages boards of directors and audit committees to monitor IT and financial risks more proactively, promoting ethical leadership and continuous improvement.

Beyond its influence on audit practices, RBISA also affects the competencies required of accounting professionals. As financial processes become more technology based, accountants need to understand IT control systems, cybersecurity principles, and data analytics. This combination of accounting and technological knowledge enables them not only to interpret audit results but also to help design secure and efficient accounting systems. With this interdisciplinary skill set, professionals can anticipate potential system risks and implement preventive measures to protect data integrity and organizational stability (Bierstaker et al., 2014).

Furthermore, the growing importance of RBISA has influenced accounting education and professional development. Universities, professional bodies, and regulators have started integrating IT auditing, risk management, and data analytics into accounting programs. Professional certifications such as CISA and CIA also emphasize risk based approaches, reflecting the evolving skills needed in modern auditing. Accountants who develop these competencies are better prepared to work in complex digital environments and provide insights that go beyond traditional financial reporting.

CONCLUSION

This paper highlights the growing importance of Risk Based Information System Auditing (RBISA) as a strategic approach to address the increasingly complex risks in the fields of accounting and information technology. In contrast to traditional audit approaches that mainly focus on following standard procedures, RBISA emphasizes the identification, analysis, and management of risks that could affect the accuracy and reliability of financial information

systems. Through structured stages such as risk identification, risk assessment, control evaluation, and reporting, RBISA ensures that audit activities are directed toward high-risk areas, especially those that have a greater potential for material misstatements, fraud, or system errors.

Based on the literature review, the integration of RBISA into accounting practices improves audit performance, strengthens internal control systems, and supports better managerial decision-making. By giving special attention to IT related controls, including user access control, data accuracy, and cybersecurity protection, RBISA helps enhance the credibility and transparency of financial reports. Furthermore, this approach promotes proactive risk management by encouraging organizations to identify potential problems early and improve their control mechanisms. This concept is consistent with governance frameworks such as COBIT, COSO, and the Sarbanes Oxley Act (SOX), which all stress the importance of risk based control systems to ensure regulatory compliance and financial responsibility.

From an accounting perspective, the adoption of Risk Based Information System Auditing (RBISA) has important consequences for both professional practice and accounting education. Today, accountants and auditors are required to have interdisciplinary abilities that combine accounting knowledge with technical skills, such as data analytics, information security, and IT governance. Mastering these skills not only enhances the quality of audits but also supports greater transparency, accountability, and trust from stakeholders.

In addition, implementing a risk-based IS audit approach helps align accounting practices with regulatory requirements. As regulatory bodies increasingly focus on the effectiveness of IT controls and cyber risk management, RBISA offers a structured method that allows organizations to prove compliance and demonstrate responsible governance. Integrating risk awareness into both auditing and accounting activities also strengthens organizational resilience, promotes ethical behavior, and supports long term sustainability.

In summary, the development of risk based IS auditing is not merely an improvement in audit procedures, but a major shift in how organizations secure and verify financial information in a digital environment. RBISA connects technological assurance with financial reliability, making the accounting profession an essential contributor to risk management and corporate governance. Continuous research and ongoing professional development are necessary to ensure that auditors and accountants are well-prepared to face future technological developments while maintaining high standards of audit quality and financial integrity.

REFERENCES

Alzeban, A., & Gwilliam, D. (2014). Factors affecting the internal audit effectiveness: A survey of the Saudi public sector. *Journal of International Accounting, Auditing and Taxation, 23*(2), 74–86. https://doi.org/10.1016/j.intaccaudtax.2014.06.001

Arena, M., & Azzone, G. (2009). Identifying organizational drivers of internal audit effectiveness. *International Journal of Auditing, 13*(1), 43–60. https://doi.org/10.1111/j.1099-1123.2008.00392.x

Bierstaker, J., Janvrin, D., & Lowe, D. J. (2014). What factors influence auditors' use of computer-assisted audit techniques? *Advances in Accounting, 30*(1), 67–74. https://doi.org/10.1016/j.adiac.2013.12.005

International Federation of Accountants. (2018). *International standards on auditing (ISAs)*. IFAC.

ISACA. (2020). *COBIT 2019 framework: Governance and management objectives*. ISACA.

Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems, 24*(1), 91–112. https://doi.org/10.2308/jis.2010.24.1.91

Lenz, R., Sarens, G., & D'Silva, K. (2014). Probing the discriminatory power of characteristics of internal audit functions: Empirical evidence. *International Journal of Auditing, 18*(2), 126–138. https://doi.org/10.1111/ijau.12016

Moeller, R. R. (2016). *Brink's modern internal auditing: A common body of knowledge* (8th ed.). Wiley.

Sari, R. N., & Nugroho, M. (2022). The role of information technology in risk-based auditing: A literature review. *Asian Journal of Accounting Research, 7*(3), 245–260. https://doi.org/10.1108/AJAR-10-2021-0204

Spraakman, G., O'Grady, W., Askarany, D., & Akroyd, C. (2015). ERP systems and management accounting: New understandings through "nudging" in research. *Journal of Accounting & Organizational Change, 11*(1), 63–88. https://doi.org/10.1108/JAOC-06-2013-0040

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2012). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting, 9*(1), 1–21. https://doi.org/10.2308/jeta-50159