Factors Affecting Information Systems Audit Conclusion

Ericky Iipumbu[1], Isaac Nhamu [2,] Mercy Chitauro [3]
[1,2,3] Namibia University of Science and Technology, Namibia

Abstract.

This paper examines the elements that significantly affect an information system audit's conclusion. The importance of guaranteeing the effectiveness, efficiency, and security of information systems has been underlined by the ongoing advancement of technology and the growing reliance on digital infrastructure. An information system audit's main goal is to assess the systems' overall integrity and to reassure stakeholders that they are trustworthy and sufficiently protected against any hazards. The paper identifies and examines the important elements that affect the outcome of information system audits by drawing on a thorough examination of the literature and empirical studies. Conducting a thorough and accurate information systems audit requires an understanding of these aspects and the proper handling of them. The results of this study give significant contributions to the field of information system auditing and provide a foundation for auditors, IT managers, and policymakers to create efficient plans for carrying out thorough and insightful audits. The ultimate goal of this article is to increase the resilience of information systems in a constantly evolving digital environment and to create a greater awareness of the elements that support audit conclusions.

Keywords: Information System Audit, Risk assessment, CIA, Internal controls.

1.0 Introduction

Modern enterprises are built on information systems, which support crucial activities and store sensitive data. Information technology is becoming more and more important, so it is crucial to examine the efficiency and security of these systems through audits. However, a number of variables can impact the findings of an information systems audit. In order to increase the dependability of audit results, this study will investigate and examine these issues.

1.1. Methodology

The review uses a systematic approach to identify relevant literature from reputable databases and publications. Selection criteria include an emphasis on information system audit (ISA), relevance to government departments, state-owned companies, and private institutions, and rigor of the research methodology. The selected works are critically analyzed and common themes and insights are worked out.

Below are the findings review on Factors Influencing Information Systems Audit Conclusion:

1.2 Audit Objectives and Scope

According to Isaca (2019) and INTOSAI (2019), audit objectives and scope have an influence on ISA conclusions. The author stated that the result of information systems audits is substantially influenced by the alignment of audit objectives and scope. Auditors can concentrate on important risk areas, vulnerabilities, and compliance requirements inside the

information systems when they have clear and appropriate audit goals. Similar to this, a clear audit scope guarantees that the audit team will evaluate the pertinent aspects and actions, preventing overlooks of important components. The audit process becomes more focused and successful when the audit objectives and scope are in line, producing accurate and pertinent conclusions and practical recommendations to improve the security, effectiveness, and dependability of information systems. The audit's overall efficacy can be hampered by misaligned objectives and scope, which can result in inadequate assessments and missed opportunities to detect potential control deficiencies the authors stated. To preserve the audit's relevance and increase its impact on information system auditing processes, flexibility in defining the audit's objectives and scope is essential as technology develops and business demands change.

1.3 Risk Assessment

Information systems audit conclusions are greatly influenced by risk assessment (Isaca, 2019; INTOSAI, 2019). Auditors can concentrate their attention and resources on the most important areas by methodically finding, assessing, and rating potential hazards within the information systems. Auditors can more effectively target their audits by understanding the underlying vulnerabilities and threats that the organization's IT environment faces with the help of a thorough risk assessment. Furthermore, the risk assessment procedure offers a foundation for evaluating the sufficiency and efficacy of current controls, enabling auditors to generate wellinformed conclusions and suggestions regarding the overall security and resilience of the information systems. As a result, a thorough risk assessment approach improves the accuracy and applicability of the audit conclusion, allowing stakeholders to learn important details about the organization's risk environment and the steps required to effectively manage possible threats.

1.4 Quality of Evidence

The outcome of the information systems audit is largely influenced by the quality of the evidence (Isaca, 2019; INTOSAI, 2019). The audit findings are guaranteed to appropriately reflect the state of the information systems by a solid and trustworthy body of evidence gathered via thorough and well-organized audit methods. Stakeholders have faith in the legitimacy of the assessment results because of the high caliber evidence supporting the audit conclusions. On the other hand, incomplete, out-of-date, or improperly gathered evidence may result in incorrect conclusions and misguided suggestions, which would compromise the audit's overall efficacy. In order to ensure that their judgments are supported by reliable facts and that companies can make informed decisions and take the necessary action to increase the security and effectiveness of their information system, auditors must highlight the quality and integrity of the evidence.

1.5 The Expertise of the Audit Team

The information systems audit's conclusion is strongly influenced by the audit team's level of knowledge (Isaca, 2019; INTOSAI, 2019). A highly competent audit team has the ability to successfully navigate complicated technical environments, pinpoint key risk areas, and thoroughly assess the effectiveness of controls. Their knowledge enables them to carry out in-depth assessments, spot minor vulnerabilities, and reach well-informed findings, which results in more accurate and pertinent audit outcomes. Additionally, seasoned auditors are better able to evaluate the data, ensuring that the assessment results are founded on a complete comprehension of the organization's particular IT environment. On the other hand, a lack of experience within the audit team could lead to risks being missed, evaluations being insufficient, and insights being limited, thereby putting the integrity and worth of the audit results in jeopardy. As a result, putting together an expert and experienced audit team is essential to producing evaluations that are meaningful and offer suggestions for improving the security, effectiveness, and overall performance of information systems.

1.6 Regulatory and Compliance Requirements:

Information systems audit conclusions are significantly influenced by regulatory and compliance requirements (Isaca, 2019; INTOSAI, 2019). In order to guarantee the security, privacy, and confidentiality of sensitive data and information, these regulations set the norms and principles that businesses must abide by. The audit team evaluates the organization's adherence to these standards during an audit to ascertain whether the information systems adhere to the relevant statutory and industry criteria. The organization has put in place the necessary controls and procedures to meet these requirements, as shown by a successful audit finding. Legal repercussions, reputational harm, or financial losses could come from noncompliance with regulations or insufficient attention to them, according to audit findings. As a result, regulatory and compliance issues are crucial in determining audit results because they encourage firms to adhere to best practices, reduce risks, and uphold stakeholders' trust by ensuring the dependability and compliance of their information systems.

1.7 Complexity of the IT Environment

The result of the information systems audit is substantially influenced by the complexity of the IT environment (Isaca, 2019; INTOSAI, 2019). Numerous interconnected systems, applications, and data repositories can provide a wide range of potential hazards and issues in complex IT ecosystems. To effectively identify crucial control points and vulnerabilities, auditors must traverse through numerous layers of technology, interfaces, and dependencies. The audit's thoroughness could also be impacted by its complexity, as some areas might be more difficult to access or comprehend. Intricate IT systems may also make it more likely that mistakes or oversights will be made throughout the audit process, which will affect how accurate the results are. To address the complexity of the IT environment, a highly qualified audit team, specialized audit methodologies, and a thorough understanding of the organization's technology infrastructure are necessary. This will ultimately improve the security, effectiveness, and resilience of the information systems.

1.8 Internal Controls

Internal controls have a significant impact on the outcome of the information systems audit(Isaca, 2019; INTOSAI, 2019). These measures are intended to protect assets, guarantee data integrity and accuracy, and stop fraudulent and unauthorized activity within the information systems. To identify the organization's risk exposure and overall security posture, the audit extensively evaluates the effectiveness and sufficiency of these measures. Strong internal controls give auditors assurance that the systems are dependable and that the data they generate is accurate. The internal controls of the corporation are effectively established, monitored, and in line with both business goals and legal requirements, according to a positive audit conclusion. The need for remedial actions to improve the governance and protection of information systems may be signaled by flaws or gaps in internal controls, on the other hand, which could result in unfavorable audit findings. As a result, the organization's capacity to protect its assets and uphold data integrity and confidentiality is directly impacted by the quality and robustness of internal controls, which also significantly affect the results of the information systems audit.

1.9 Data Quality

A significant component affecting the outcome of the information systems audit is data quality (Isaca, 2019; INTOSAI, 2019). The validity of audit findings and the efficacy of control evaluations are directly impacted by the correctness, completeness, and reliability of data within the systems. Auditors need high-quality data to make wise decisions and precise assessments of the organization's IT infrastructure, risks, and controls. On the other hand, bad data quality might produce false suggestions, overlooked vulnerabilities, and incorrect conclusions. Data is used by auditors to spot patterns, trends, and anomalies as well as to confirm the efficacy of controls and regulatory compliance. As a result, businesses must give data quality management top priority because it immediately improves the validity and applicability of the audit conclusions, empowering stakeholders to take well-informed actions to increase the security and operational effectiveness of information systems.

1.10 Discussion

Despite the factors affecting the conclusion of the information systems audit, the discussion on how to improve the information systems audit (ISA) is still ongoing to improve the whole ISA process to ensure a high-quality conclusion from the audit, which leads to good recommendations for improving organizations' IT infrastructures and ensuring confidentiality, integrity, and availability (CIA) of data. Other streams of audit also rely on internal controls tested by information systems auditors. When assessing the standard of information systems auditing, three studies in particular (Stoel et al. (2012), Havelka & Merhout (2013), and Putri & Mardijuwono 2020, as cited in Alagi, Turulja & Bajgori, 2021) stand out, and no measuring scale has been adopted, even though these authors discussed the subject of information systems auditing quality. Moreover, the current auditing models are insufficient to be applied in practice due to the complexity of modern IT Systems and their inability to detect

sophisticated cyber threats, and the limited ability to analyze large amounts of data in different formats, which have led to the rise in cybercrime, and data breaches (Siponen & Vance, 2010; Alexiou, 2019; Nabil, 2021; Youngjoo and Sooyong, 2021; Martin et al., 2022).

1.11 Conclusion

The results of the audit of information systems clearly illustrate the complex interaction of numerous influencing factors. Every aspect affects the accuracy, reliability, and relevance of audit results, from the definition of precise audit objectives and scope to the competence of the audit team, from the rigor of risk assessment to the robustness of internal controls. The complexity of the technology, regulatory compliance, and data quality all add to the complexity of this process. The convergence of these variables underscores the need for an all encompassing approach to auditing information systems. Organizations need to proactively address these different dimensions to ensure audit conclusions are both meaningful and actionable. This includes continually adjusting audit objectives and scope, building an experienced and competent audit team, managing changing technical environments, and promoting a data quality management culture. By understanding the complex interplay and value of these factors. Additionally, Information systems auditing (ISA) is a critical process in business informatics. However, the process and tools used are not enough to detect complex cyber threats. As a result, there can be undetected security breaches, compromised data confidentiality, integrity, and availability, and an increased risk of cyberattacks. This can affect the overall effectiveness of the ISA process and the validity of evidence collected by IS auditors, potentially leading to inaccurate system assessments.

References

Alagić, A., Turulja, L., & Bajgorić, N. (2021). Identification of Information System Audit Quality Factors. Journal of Forensic Accounting Profession, 1(2), 1–28 https://doi.org/10.2478/jfap-2021-0006

Alexiou, S. (2019, November 1). Trends, Challenges, and Strategies for Effective Audit in a Rapidly Changing Landscape. *ISACA*. Retrieved March 21, 2023,from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/trends challenges-and-strategies-foreffective-audit-ina-rapidly-changing-landscape

INTOSAI. (2019). GUID INTOSAI 5100 Guidance on Audit of Information Systems. https://www.issai.org/wp-content/uploads/2019/09/Guid5100-Guidance -on-Auditof-Information-Systems.pdf Isaca. (2019). *CISA Review Manual* (27th ed.). ISACA.

Martin. C, CISA, CISSP [ISO/IEC 27001 LA], and PCI QSA (2022) *An Integrated Approach to Security Audits*. Available at: https://isaca.org/resources/news-and-trends/industry

news/2022/anintegratedapproach-to-security-audits (Accessed: May 20, 2023).

Nabil, F. (2021, November 13). The role of information technology in improving auditing quality and reporting at the State Audit Bureau of Kuwait. *Https://Ligsuniversity.Com/*. Retrieved March 21, 2023, from https://ligsuniversity.com/blog/the-role-ofinformation-technology-inimproving-auditing-quality-and-reporting-at-the-stateaudit-bureau-ofkuwait

Siponen, M. T., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *Management Information Systems Quarterly*, *34*(3), 487. https://doi.org/10.2307/25750688

Youngjoo, L., & Sooyong, P. (2021). Technology-based Practical Blockchain System Audit Maturity Model. *Tehnički Vjesnik*, *28*(2), 576–586.