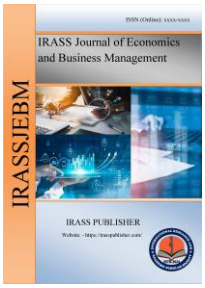
IRASS Journal of Economics and Business Management
Abbriviate Title- IRASS J Econ Bus Manag
ISSN *(Online) xxxx-xxxx*
https://irasspublisher.com/journal-details/IRASSJEBM
Vol-1, Iss-1(December-2024)



Implementation of Information Technology Audit in Improving Company Operational Security and Efficiency

Bill Cheristian Sebayang[1*], Crisanto William[2], Iskandar Muda[3], Gusnardi[4]

[*1-2-3]Universitas Sumatera Utara, Medan, Indonesia

[4] Universitas Riau, Pekanbaru, Indonesia

Corresponding Author **Bill Cheristian Sebayang**

Universitas Sumatera Utara, Medan, Indonesia

Article History

Received: 22 / 11/ 2024

Accepted: 12 / 12 / 2024

Published: 14 / 12 / 2024

Abstract: The rapid development of information technology (IT) has encouraged companies to adopt IT audits to improve information security and operational efficiency. IT audits are important to ensure that a company's IT systems operate safely and in accordance with applicable standards, such as COBIT and ISO 27001. This study uses a mixed method approach that combines qualitative and quantitative methods. Data were collected through in-depth interviews with auditors and IT managers and questionnaires distributed to 100 companies in Indonesia that have implemented IT audits for at least two years. Qualitative analysis was conducted using thematic methods, while quantitative data were analyzed using descriptive statistics, Pearson correlation, and linear regression. The results showed that the implementation of IT audits contributed to increased information security, with 85% of companies reporting a reduced risk of data breaches. In addition, 78% of companies stated that IT audits also improved operational efficiency, such as reduced downtime and improved system management. These findings underscore the importance of IT audits as a strategic tool in managing risk and improving company performance in the digital era.

Keywords: Information technology audit, information security, operational efficiency.

Introduction

In the rapidly developing digital era, the application of information technology (IT) has become the main foundation for the operations of various companies. The use of technology, such as cloud computing, Enterprise Resource Planning (ERP) systems, mobile device management (MDM), and the Internet of Things (IoT), allows companies to manage large amounts of data more efficiently and in real time (Rajesh et al., 2022). However, along with this progress, the risks associated with information security and cyber threats have also increased significantly. Therefore, the implementation of information technology audits (IT audits) is becoming increasingly important as a tool to ensure that the IT systems used by companies are not only efficient, but also safe from threats that can disrupt company operations (Henderson et al., 2013, Khan ET AL., 2023) .

IT audit is the process of evaluating the IT infrastructure in a company, including hardware, software, networks, and security procedures implemented. This audit aims to assess the effectiveness of implemented security controls and policies, and ensure that all IT components are operating according to established standards. Furthermore, IT audits also help companies identify weaknesses that can be exploited by unauthorized parties to access critical data, allowing companies to take better preventive measures. (Moorthy et al., 2011) .

IT audits contribute greatly to improving efficiency by optimizing the use of existing technology. Through audits, companies can identify areas that require technology upgrades or updates to ensure that the system is working optimally. In addition, IT audits also help ensure that the use of technology is in accordance with applicable regulations, thereby avoiding potential legal issues in the future. Thus, the implementation of IT audits is a crucial step in creating a safe, efficient, and regulatory-compliant operational environment, which will ultimately improve the overall performance of the company (Abu-Musa, 2008) .

IT audits also enable companies to identify and manage risks associated with technology. By conducting regular evaluations of IT security systems and infrastructure, audits can detect vulnerabilities that could be exploited by unauthorized parties (Asniarti, 2019). This helps companies take preventive measures, such as improving access control, updating security software, or strengthening data encryption protocols. In this way, the risk of cyberattacks and data leaks can be minimized, which has an impact on increasing customer and business partner trust.

IT audits also play a role in optimizing operational costs. By identifying inefficient systems or outdated technology, companies can allocate resources more appropriately. For example, legacy systems that require high maintenance costs can be replaced with more modern and efficient technology. This not only reduces costs

but also speeds up business processes, so that response time to customer needs can be improved (Prabowo, 2024)

IT audits also play an important role in helping companies comply with various standards and regulations, such as ISO 27001, COBIT, and GDPR (General Data Protection Regulation). Compliance with these regulations is not only important to avoid legal sanctions, but can also improve the company's reputation in the eyes of customers and investors. With a better reputation, companies have the opportunity to expand their markets and increase their competitiveness (Alrawashedh, 2022) .

Literature Review

Information Technology Audit Concept

Information technology audit is a process carried out to evaluate IT infrastructure, systems, and controls within a company. According to Otero (2018) in his book *Information Technology Control and Audit* , IT audits aim to ensure that the technology used by the company is functioning properly, is safe from external threats, and complies with applicable regulations. This includes examining various aspects such as access control, data integrity, and operational sustainability. IT audits also help identify technology risks that can threaten information security and reduce company productivity. (Otero, 2018) .

IT Audit Standards

Several IT audit standards have been developed to ensure that audit processes are carried out consistently and with quality. One widely used standard is COBIT (Control Objectives for Information and Related Technologies), which provides a framework for the governance and management of enterprise information technology. COBIT emphasizes the importance of alignment between business and IT strategies, and ensures that all technology processes within the company support the achievement of business objectives. In addition to COBIT, ISO/IEC 27001 is also a widely used standard in ensuring effective information security management within an organization.

According to Chinedu et al. (2019), the implementation of these standards provides a clear framework in the audit process, so that auditors can identify ineffective controls and provide recommendations for necessary improvements. This is very important in mitigating security risks and increasing the efficiency of technology processes (Stoel et al., 2012) .

The Role of IT Audit in Information Security

Information security is one of the main focuses of IT audits. As companies increasingly rely on technology to carry out their daily operations, threats to data security continue to increase. A study by Luo and Oliva (2008) showed that companies that routinely conduct IT audits have better levels of information security, because audits help identify potential vulnerabilities before they become serious threats. The audit process provides companies with insight into system weaknesses that can be fixed through improved access controls, data encryption, and the implementation of better risk management policies (Vrontis et al., 2021) .

IT Audit and Operational Efficiency

In addition to its role in security, IT audits have also been shown to contribute to improving a company's operational efficiency. Research conducted by Prasad et al. (2020) revealed that IT audits enable companies to identify systems or processes that are outdated or less efficient. By conducting regular audits, companies can make necessary technology updates and optimize the use of existing resources, thereby increasing productivity and reducing operational costs.

Challenges in IT Audit Implementation

Although IT audits provide many benefits, their implementation also faces various challenges. One of the main challenges is the lack of auditors who have in-depth knowledge of the latest technologies. Otero (2018) underlines the importance of auditors to continuously update their knowledge in order to conduct audits effectively in an ever-evolving technological environment. In addition, the integration of audits with business strategies is also often an obstacle, especially for companies that do not have adequate resources to manage complex audit processes. (MAHZAN & HASSAN, 2015) .

Methods

This study uses a mixed qualitative and quantitative approach. Data were collected through interviews with IT auditors and IT managers, as well as questionnaires distributed to 100 companies in Indonesia that have implemented IT audits for at least two years. Secondary data from audit reports and previous studies were also used. Qualitative analysis was conducted using thematic methods, while quantitative analysis used descriptive statistics, Pearson correlation, and linear regression to see the relationship between IT audits and security and operational efficiency. Data validity was tested through triangulation and questionnaire reliability was tested using *Cronbach's Alpha* . Research limitations include limited data access and regional focus in Indonesia.

Results and Discussion

Results

This study successfully collected data from 100 companies in Indonesia that have implemented information technology (IT) audits for at least two years. Based on the analysis of questionnaire data distributed to respondents, it was found that 85% of companies stated that the implementation of IT audits had contributed significantly to improving their information security. In addition, 78% of companies also reported an increase in operational efficiency after conducting regular audits. This data shows a strong relationship between the implementation of IT audits and improvements in security systems and business operations.

In terms of information security, companies that routinely conduct IT audits report a decrease in data security breach incidents. As many as 70% of respondents stated that after the audit, they were able to identify and fix weaknesses in the security system that were previously undetected. In addition, 68% of companies reported a decrease in the risk of data leakage after implementing audit recommendations. This indicates that IT audits play an important role in maintaining the integrity and confidentiality of company information.

The results of the study showed that companies that routinely conduct IT audits experience an increase in data processing speed and IT infrastructure management. As many as 75% of companies reported significant improvements in IT system management, such as improvements in server, network, and application management.

In addition, 64% of respondents stated that IT audits helped them reduce downtime or unproductive time due to technical problems, which ultimately increased company productivity.

Linear regression analysis conducted shows a significant positive relationship between the implementation of IT audit with information security and operational efficiency. The regression coefficient shows a positive value of 0.62 for the information security variable and 0.58 for the operational efficiency variable, which means that any increase in the implementation of IT audit will be followed by an increase in security and efficiency simultaneously.

Interviews with internal and external auditors found that IT audits help companies identify gaps in access control settings, data encryption, and cybersecurity risk management. Auditors also reported that companies that conduct regular audits are better prepared for cyber threats and are quicker to respond to security incidents.

These results show that the implementation of IT audits not only impacts information security but also contributes to overall operational improvements, including technology resource management and operational efficiency. In addition, audits also help companies to be more compliant with applicable regulations and standards, such as COBIT and ISO 27001, which contribute to the achievement of greater business goals.

Discussion

The findings of this study emphasize the importance of IT audits as a key element in managing the security and operational efficiency of a company. From the results obtained, it can be seen that IT audits play an important role in minimizing information security risks through early identification of system weaknesses. IT audits enable companies to detect and fix previously unidentified problems, such as errors in access control settings or lack of adequate encryption management policies. This is in line with research conducted by Luo and Oliva (2008), which found that companies that routinely conduct IT audits have lower security risks compared to companies that do not conduct audits.

The importance of implementing standards such as COBIT and ISO 27001 in IT audits is also reflected in the findings of this study. These standards provide a clear framework for auditors to evaluate a company's IT systems and help ensure that the company adheres to best practices in information management. For example, implementing COBIT allows companies to align their IT strategies with business objectives more effectively. This supports the research of Chinedu et al. (2019), which shows that companies that adopt IT audit standards tend to be more successful in optimizing their resources and reducing operational risks.

ISO 27001 provides comprehensive guidance for information security management, including risk management and data protection. Implementing this standard helps companies maintain the confidentiality, integrity, and availability of information. With ISO 27001, companies can develop policies and procedures that ensure that access to data is granted only to authorized parties, thereby reducing the risk of data leakage or privacy breaches. Effective implementation of this standard also strengthens the trust of third parties, such as clients and business partners, in the security of information managed by the company.

By following the framework provided by these standards, companies can better prepare themselves for external audits or certifications required to meet regulatory requirements across industries. It also helps companies identify areas that need improvement before bigger problems arise. Thus, implementing standards such as COBIT and ISO 27001 is not just about compliance, but also about creating IT systems that are more efficient, secure, and aligned with the company's strategic goals.

This discussion highlights how IT audits can help companies improve operational efficiency. As the research findings show, IT audits not only help improve information security but also contribute to improving overall IT system management. In many cases, companies that have implemented regular audits have been able to reduce downtime and improve their technology infrastructure, thereby increasing productivity and reducing operational costs. Research by Prasad et al. (2020) also supports this finding, where companies that conduct regular IT audits are able to identify and fix inefficient systems, thereby improving their operational output.

There are several challenges that companies face in implementing IT audits effectively. One of the main challenges is limited resources, both in terms of trained auditors and the budget available for audits. Otero (2018) noted that many companies, especially small and medium-sized companies, have difficulty setting aside a budget for a comprehensive IT audit. In addition, companies often do not have in-depth knowledge of the latest technologies, making it difficult for them to fully utilize the benefits of an IT audit.

Despite these challenges, IT audits are still considered an important investment by many companies. The findings suggest that while the initial cost of an audit can be high, the long-term benefits in reducing security risks, increasing efficiency, and complying with regulations far outweigh the benefits. Therefore, companies need to view IT audits as an integral part of their risk management and technology governance strategies.

This study confirms that IT audits are not only a tool to ensure compliance with standards and regulations, but also have a strategic role in supporting the achievement of business goals. By identifying risks early and ensuring that IT systems are operating efficiently, companies can achieve a competitive advantage in this digital era. Companies that continue to innovate in IT audit practices will be better prepared to face future technological challenges, including cyber threats and increasingly complex regulatory changes.

IT audits provide valuable insights into the optimization of resources, enabling companies to allocate investments in technology more effectively. Through regular auditing, companies can avoid costly downtime, enhance productivity, and ensure that critical IT infrastructure supports long-term business growth. This proactive approach also strengthens cybersecurity measures, reducing vulnerabilities and enhancing data protection, which is crucial in maintaining the trust of clients, partners, and stakeholders.

As the business environment evolves, those organizations that integrate IT audit into their strategic planning will be better positioned to adapt and innovate. This agility not only ensures resilience in the face of technological disruption but also aligns IT

objectives with broader business goals. In turn, this alignment fosters improved decision-making, enhances operational performance, and ultimately drives sustainable growth and success in the competitive marketplace.

Conclusion

This study shows that the implementation of information technology (IT) audits plays an important role in improving information security and operational efficiency of companies. Based on the results obtained, companies that routinely conduct IT audits experience a decrease in information security risks, such as data leaks and access violations, as well as increased efficiency in managing IT infrastructure, which has a direct impact on productivity and reduced operational costs.

IT audits have been shown to help companies identify weaknesses in security systems, such as inadequate access control settings and data encryption, and facilitate IT infrastructure improvements to reduce downtime. The use of IT audit standards such as COBIT and ISO 27001 has also been shown to be effective in ensuring regulatory compliance and improving the alignment of IT strategy with a company's business objectives.

Although there are challenges in implementing IT audits, especially related to resources and costs, the long-term benefits of these audits are much greater in terms of risk reduction, increased productivity, and legal compliance. Therefore, IT audits should be seen as a strategic investment that supports the sustainability and competitiveness of companies in the digital era. The implementation of IT audits is a crucial step in building a safe, efficient, and regulatory-compliant operational environment, which ultimately contributes to the success and sustainability of the company.

References

1. Abu-Musa, AA (2008). Information technology and its implications for internal auditing: An empirical study of Saudi organizations. *Managerial Auditing Journal* , *23* (5), 438–466. https://doi.org/10.1108/02686900810875280
2. Alrawashedh, N.H. (2022). Role of Information Technology in improving the work of External Auditors, A Study of Jordan. *Central European Management Journal* , *November* . https://doi.org/10.57030/23364890.cemj.30.4.155
3. Asniarti, A., (2019). The Effect of Computer Assisted Audit Tools on Operational Review of Information Technology Audits. In *1st International Conference on Social Sciences and Interdisciplinary Studies (ICSSIS 2018)*. Atlantis Press. https://doi.org/10.2991/icssis-18.2019.5
4. Henderson, D. L., Davis, J. M., & Lapke, M. S. (2013). The Effect of Internal Auditors' Information Technology Knowledge on Integrated Internal Audits. *International Business Research* , *6* (4), 147–163. https://doi.org/10.5539/ibr.v6n4p147
5. Khan, S. I., Kaur, C., Al Ansari, M. S., , Borda, R. F. C., & Bala, B. K. (2023). Implementation of cloud based IoT technology in manufacturing industry for smart control of manufacturing process. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, 1-13. https://doi.org/10.1007/s12008-023-01366-w
6. MAHZAN, N., & HASSAN, NAB (2015). Internal Audit of Quality in 5s Environment: Perception on Critical Factors, Effectiveness and Impact on Organizational Performance. *International Journal of Academic Research in Accounting, Finance and Management Sciences* , *5* (1). https://doi.org/10.6007/ijarafms/v5-i1/1471
7. Moorthy, M. K., Seetharaman, A., Mohamed, Z., Gopalan, M., & Lee, H. S. (2011). The impact of information technology on internal auditing. *African Journal of Business Management* , *5* (9), 3523–3539. https://doi.org/10.5897/AJBM10.1047
8. Otero, A. R. (2018). Information Technology Control and Audit. In *Information Technology Control and Auditing* . https://doi.org/10.1201/9780429465000
9. Prabowo, WA (2024). Developing Compliant Audit Information System for Information Security Index: A Study on Enhancing Institutional and Organizational Audits Using Web-based Technology and ISO 25010:2011 Total Quality of Use Evaluation. *International Journal on Informatics Visualization* , *8* (1), 343–351. https://doi.org/10.62527/joiv.8.1.1845
10. Rajesh, S., Abd Algani, Y. M., Al Ansari, M. S., Balachander, B., Raj, R., & Balaji, S. (2022). Detection of features from the internet of things customer attitudes in the hotel industry using a deep neural network model. *Measurement: Sensors*, 22, 100384. https://doi.org/10.1016/j.measen.2022.100384.
11. Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems* , *13* (1), 60–79. https://doi.org/10.1016/j.accinf.2011.11.001
12. Vrontis, D., Karagiorgos, A., Thrassou, A., Drogalas, G., & Lois, P. (2021). Internal auditing and cyber security: audit role and procedural contribution. *International Journal of Managerial and Financial Accounting* , *13* (1), 25. https://doi.org/10.1504/ijmfa.2021.10039257