Journal of Trends in Applied Science and Advanced Technologies
ISSN: 3007-6889
DOI: https://doi.org/10.61784/asat3007

THE ROLE OF IT AUDITING IN DATA SECURITY FOCUSING ON RISK IDENTIFICATION, STRENGTHENING INTERNAL CONTROLS, AND COMPLIANCE WITH SECURITY POLICIES

Indy Misya Rumata Situmorang, Kania Jasmine Azzahra, Iskandar Muda*
Universitas Sumatera Utara, Medan, Indonesia.
Corresponding author: Iskandar Muda, Email: ismuda.jurnal.internasional@gmail.com

Abstract: In an increasingly digital era, data security has become one of the top priorities for organizations. Information Technology (IT) auditing plays a crucial role in ensuring that the information systems and data managed by companies are protected from potentially harmful threats. This paper aims to explore the role of IT auditing in enhancing data security, focusing on risk identification, strengthening internal controls, and compliance with security policies. Through a qualitative approach, this research collects data from interviews with audit professionals and case studies from several organizations. The results indicate that IT auditing not only helps identify weaknesses in security systems but also provides recommendations that can enhance data protection effectiveness. Additionally, IT auditing contributes to raising awareness of the importance of data security throughout the organization. The conclusion emphasizes that the routine implementation of IT auditing is a strategic step necessary to maintain the integrity and confidentiality of information in an increasingly complex business environment. This abstract provides a brief summary of the objectives, methodology, results, and conclusions of the research regarding the role of IT auditing in data security.

Keywords: IT audit; Data security; Risk management; Internal controls; Compliance; Vulnerabilities; Information protection; Information systems; Data breach

1 INTRODUCTION

In an increasingly advanced digital era, organizations face various challenges related to data security. With the growing volume of data generated and stored, as well as the complexity of the information systems used, the risks of data breaches, cyberattacks, and information misuse are becoming increasingly significant [1]. Data security is not only essential for protecting sensitive information but also for maintaining the reputation and trust of customers. In this context, Information Technology (IT) auditing emerges as a crucial tool for assessing and enhancing data security within organizations. IT auditing serves to evaluate the effectiveness of existing internal controls, identify potential risks, and ensure that security policies and procedures are properly followed [2]. Through a systematic audit process, organizations can gain better insights into their security system's strengths and weaknesses. However, despite the recognized importance of IT auditing, many organizations have yet to implement audit practices routinely or effectively. This research aims to:

1. Identify the Role of IT Auditing: Explain how IT auditing contributes to enhancing data security within organizations.
2. Analyze the Audit Process: Examine the steps taken in IT auditing to identify and address data security risks.
3. Provide Recommendations: Develop recommendations for best practices in the implementation of IT auditing to improve data protection.
4. Increase Awareness: Enhance understanding of the importance of IT auditing in the context of information security among professionals and stakeholders.

2 LITERATURE REVIEW

2.1 Definition of IT Audit

An Information Technology (IT) audit is the process of evaluating an organization's information technology systems, infrastructure, and policies. The purpose of this audit is to ensure that all aspects of IT operate in accordance with established security and efficiency standards [2]. IT audits encompass reviews of hardware, software, as well as procedures and policies related to data management and information systems within the organization. By conducting an IT audit, organizations can identify potential risks, weaknesses in internal controls, and ensure compliance with applicable regulations.

2.2 Objectives of IT Audit

The primary objectives of an IT audit include [3]

1. Risk Identification: Identifying potential security risks that may threaten data and information systems.
2. Performance Assessment: Evaluating the performance of IT systems to ensure they function effectively and efficiently.

3. Regulatory Compliance: Ensuring that all IT policies and procedures comply with relevant regulations and standards.
4. Improvement Recommendations: Providing recommendations for improvements based on audit findings to enhance the security and efficiency of systems.

2.3 Commonly Used Methodology

The methodology for IT auditing generally follows these steps: [3]
1. Audit Planning: This step involves determining the scope, objectives, and approach of the audit. At this stage, auditors need to understand the information technology assets present in the organization.
2. Data Collection: Information regarding the IT systems is gathered through interviews, document reviews, and direct observations to gain an in-depth understanding of the technologies used.
3. Control Evaluation: This involves testing the effectiveness of security controls and procedures implemented within the IT systems. It includes analyzing security mechanisms and assessing potential weaknesses.
4. Findings Analysis: Analyzing findings related to control weaknesses and evaluating the risks faced by the organization based on the evaluation results.
5. Audit Reporting: Compiling a report that summarizes the evaluation results and improvement recommendations. The report should be clear and easily understood, serving as a strategic guide for the organization.
6. Follow-Up: Ensuring that recommendations are effectively implemented and monitoring to assess the effectiveness of changes made.

2.4 Data Security: Explanation, Threats, and Importance of Data Protection

2.4.1 Explanation of data security
Data security refers to practices designed to protect digital data and information from unauthorized access, misuse, or theft. It encompasses a series of steps and technologies aimed at maintaining the confidentiality, integrity, and availability of data throughout its lifecycle [4]. Data security involves understanding the types of data held, their storage locations, and the risks that threaten that data. With the increasing reliance on technology and the internet, data security has become crucial for protecting sensitive information from existing threats.

2.4.2 Existing threats
Threats to data security can arise from various sources, including:
1. Cyber Attacks: Such as malware, ransomware, phishing, and Distributed Denial of Service (DDoS) attacks that can damage or steal data.
2. Unauthorized Access: Unauthorized users may attempt to access sensitive data illegally.
3. Data Breaches: Occur when sensitive information leaks to third parties without permission, often due to human error or system failures.
4. Physical Damage: Loss of data due to natural disasters or hardware failures also poses a serious threat to data security.

These threats can lead to significant financial losses for organizations and damage their reputation in the eyes of customers and business partners.

2.4.3Importance of data protection
Data protection is crucial for several reasons: [2]
- Protecting Individual Privacy: Data security helps safeguard personal information from falling into the wrong hands, thereby protecting individual privacy.
- Maintaining Business Integrity: Organizations that can effectively protect their data are more likely to gain the trust of customers and business partners, which in turn enhances the company's reputation.
- Preventing Financial Loss: Data breaches or losses can result in significant financial repercussions due to legal penalties, loss of customers, and recovery costs.
- Compliance with Regulations: Many countries have laws and regulations that require organizations to protect personal data. Failure to comply with these regulations can lead to legal sanctions.

2.5 The Relationship Between IT Audit and Data Security

Information Technology (IT) auditing plays a crucial role in enhancing data security within organizations. In this context, IT audits serve not only as tools to assess compliance with policies and procedures but also as mechanisms to identify and mitigate potential risks that could threaten the integrity and confidentiality of data [5]. The following points illustrate the relationship between IT auditing and improved data security:
1. Evaluation of Security Weaknesses: IT audits conduct in-depth assessments of IT systems to identify vulnerabilities in data security. As noted in literature, IT audit services can assist organizations in detecting vulnerabilities to cyberattacks, such as hacking and malware, which can compromise sensitive data. By performing these evaluations, auditors can provide recommendations to strengthen security infrastructure.
2. Enhancement of Security Infrastructure: After identifying weaknesses, IT audits play a role in providing recommendations for improving security infrastructure. This includes enhancements to firewalls, data encryption, and

critical software updates. By implementing these measures, organizations can reduce the risks of data breaches and cyberattacks.

3. Regulatory Compliance: IT audits also ensure that organizations comply with applicable data protection regulations, such as GDPR or Indonesia's Personal Data Protection Law. Adhering to these regulations not only helps avoid significant fines but also enhances customer trust in the organization. Regular audits can assist organizations in maintaining this compliance.
4. Monitoring and Early Detection: IT audits aid in establishing effective monitoring systems to detect suspicious activities or security threats early on. With early detection, preventive actions can be taken before an attack occurs, thereby better safeguarding data security.
5. Preventing Data Breaches: Through regular audits, organizations can prevent data breaches before they happen. The audit process helps identify security gaps that could be exploited by cybercriminals and provides improvement recommendations to mitigate the risk of reputational damage or financial loss due to security incidents.
6. Increasing Security Awareness: IT audits also serve to raise awareness about the importance of information security throughout the organization. By involving all employees in the audit process and providing training on security policies, organizations can foster a stronger culture of security.

Overall, the relationship between IT auditing and data security is very close. Through systematic evaluations and improvement recommendations provided by IT auditors, organizations can enhance their data protection levels and minimize risks associated with cyber threats [6]. Thus, IT auditing becomes an integral part of risk management strategies and data protection in today’s digital era.

3 METHODS

3.1 Research Design

This research employs a qualitative approach to explore the role of IT auditing in enhancing data security within organizations. The qualitative approach is chosen because it allows the researcher to gain an in-depth understanding of the phenomena being studied, as well as the context and dynamics influencing the implementation of IT audits and data security.

Reasons for Choosing a Qualitative Approach

1. Depth of Information: The qualitative approach enables researchers to delve deeply into information through interviews and focus group discussions. This provides richer insights into the experiences and perspectives of IT audit and data security professionals.
2. Flexibility: Qualitative methods offer flexibility in data collection, allowing researchers to adjust questions and research focus based on participant responses.
3. Concepts and Perceptions: This research aims to understand the concepts and perceptions held by practitioners regarding the relationship between IT auditing and data security, which can be better explored through a qualitative approach.

3.2 Data Collection Methods

1. In-Depth Interviews: The researcher will conduct interviews with professionals involved in IT auditing and data security across various organizations. These interviews will be semi-structured, allowing the researcher to have a set of questions while also being open to further discussion based on the respondents' answers.
2. Case Studies: This research will also include case studies from several organizations that have effectively implemented IT audits. These case studies will provide real-world examples of how IT auditing contributes to enhancing data security.
3. Document Analysis: In addition to interviews and case studies, the researcher will analyze relevant documents, such as previous audit reports, data security policies, and internal procedures of the organizations. This will help provide additional context and support the findings from the interviews.

3.3 Data Analysis

The data collected through interviews and document analysis will be analyzed using thematic analysis techniques. This process involves identifying patterns, themes, and categories that emerge from the data to address the research questions. The results of this analysis will be used to formulate key findings regarding the role of IT auditing in enhancing data security.With this qualitative approach, the research aims to provide a deeper understanding of how IT auditing can contribute to data protection within organizations, as well as the challenges and opportunities encountered during its implementation.

4 RESULTS AND DISCUSSION

4.1 Results

This research identifies several key findings related to the role of Information Technology (IT) auditing in enhancing data security within organizations. Based on data analysis obtained from interviews, case studies, and relevant literature, here is a summary of the main findings:

1. Identification of Security Weaknesses: IT audits effectively identify weaknesses in security systems that organizations may not be aware of. For instance, an audit conducted at Institution X using the ISO/IEC 27002 standard revealed vulnerabilities in access management and data protection that could be exploited by unauthorized parties. By identifying these weaknesses, organizations can take necessary corrective actions.
2. Enhancement of Security Infrastructure: After weaknesses are identified, IT audits provide recommendations for improving security infrastructure. These recommendations may include enhancements to firewalls, implementation of data encryption, and critical software updates [7]. The research found that organizations implementing audit recommendations experienced significant improvements in their data security levels.
3. Early Detection of Security Threats: IT audits assist organizations in establishing effective monitoring systems to detect suspicious activities or security threats early on. With early detection, preventive actions can be taken before attacks occur. This was evidenced in a case study at PT Paramita Surya Makmur Plastika, where the implementation of monitoring systems resulting from audits successfully prevented several security incidents.
4. Compliance with Regulations: IT audits also ensure that organizations comply with applicable data protection regulations, such as GDPR and Indonesia's Personal Data Protection Law. The research indicates that companies conducting regular audits are better positioned to meet regulatory requirements and avoid legal sanctions.
5. Increased Security Awareness: IT audits contribute to raising awareness about the importance of data security throughout the organization. Through training and employee involvement in the audit process, organizations can create a stronger security culture.

4.2 Analysis of the Role of IT Audit

IT auditing plays a crucial role in helping organizations identify risks, enhance controls, and ensure compliance with security policies [8]. The following is a further analysis of these roles:

- Risk Identification: During the audit process, auditors evaluate the security systems and risk management practices implemented by the organization. By identifying potential risks such as software vulnerabilities or weak access policies, auditors provide valuable information to management for taking corrective actions. This proactive identification helps organizations mitigate risks before they can be exploited.
- Enhancing Controls: IT audits strengthen internal controls by providing recommendations for best practices in data and information system management. For instance, implementing role-based access control (RBAC) and data encryption can significantly enhance the protection of sensitive information. The recommendations from audits help organizations establish a more robust security framework.
- Ensuring Compliance: By ensuring that security policies and procedures are adhered to, IT audits assist organizations in meeting regulatory requirements and industry standards. This not only protects organizations from legal sanctions but also enhances stakeholder confidence in the organization's ability to manage data effectively. Regular audits help maintain compliance with regulations such as GDPR and HIPAA.

4.3 Case Study

As a real world example of the implementation of IT auditing, this research includes a case study at Institution X, which conducted a security audit using the ISO/IEC 27002 and COBIT 5 standards. The audit results indicated that the maturity level of IT at the institution was at level 2 (Managed Process), meaning that the processes for implementing information technology had been carried out in a more organized manner but still required improvements.After implementing the recommendations from the audit, which included enhancements to access controls and updates to security procedures, Institution X reported a significant decrease in data breach incidents and an increase in user satisfaction with their services. This case study underscores that the routine implementation of IT auditing not only enhances data security but also provides operational benefits for organizations.

5 CONCLUSION

This research highlights the critical role of Information Technology (IT) auditing in enhancing data security within organizations. Through a systematic approach, IT audits enable organizations to identify vulnerabilities in their security systems, strengthen internal controls, and ensure compliance with relevant regulations. The findings indicate that effective IT auditing leads to several key outcomes:

1. Identification of Security Weaknesses: IT audits provide organizations with insights into potential vulnerabilities that may go unnoticed, allowing for timely corrective actions.
2. Enhancement of Security Infrastructure: By implementing recommendations from audits, organizations can significantly improve their security measures, including access controls and data protection protocols.
3. Early Detection of Threats: IT audits facilitate the establishment of effective monitoring systems that help detect suspicious activities early, enabling proactive responses to potential security incidents.
4. Regulatory Compliance: Regular audits ensure that organizations adhere to data protection regulations such as GDPR and the Personal Data Protection Law in Indonesia, thereby avoiding legal penalties and fostering stakeholder

trust.

5. Increased Awareness of Data Security: Engaging employees in the audit process and providing training on security policies contribute to a stronger culture of data security within organizations.

By adopting these practices, organizations can fortify their data security measures and protect their information assets against various digital threats. Ultimately, integrating IT auditing into organizational strategies is essential for effective risk management and ensuring the long-term security of sensitive data.

CONFLICT OF INTEREST

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Shulha, O, Yanenkova, I, Kuzub, M, et al. Modeling Regarding Detection of Cyber Threats Features In Banks Activities. Journal of Management Information & Decision Sciences, 2022, 25(25): 1-8.

[2] Demirkan, S, Demirkan, I, McKee, A. Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 2020, 7(2): 189-208.

[3] Lois, P, Drogalas, G, Karagiorgos, A, Tsikalakis, K. Internal audits in the digital era: opportunities risks and challenges. EuroMed Journal of Business, 2020, 15(2): 205-217.

[4] AlGhamdi, S, Win, K T, Vlahu-Gjorgievska, E. Information security governance challenges and critical success factors: Systematic review. Computers & security, 2020, 99, 102030.

[5] Yang, P, Xiong, N, Ren, J. Data security and privacy protection for cloud storage: A survey. Ieee Access, 2020, 8, 131723-131740.

[6] Wylde, V, Rawindaran, N, Lawrence, J, et al. Cybersecurity, data privacy and blockchain: A review. SN computer science, 2022, 3(2): 127.

[7] Bandari, V. Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. International Journal of Business Intelligence and Big Data Analytics, 2023, 6(1): 1-11.

[8] Duggineni, S. Impact of controls on data integrity and information systems. Science and Technology, 2023, 13(2): 29-35.