JOURNAL OF MANAGEMENT, ACCOUNTING, GENERAL FINANCE AND INTERNATIONAL ECONOMIC ISSUES
(MARGINAL)

CONCEPT AND APPLICATION OF AUDIT IN INFORMATION SYSTEMS

Masnawaty Sangkala
Accounting Study Program, Faculty of Economics and Business, Universitas Negeri Makassar
E-mail: masnawaty.s@unm.ac.id

Abstract

The motivation behind this research lies in the critical role of sophisticated information systems in financial auditing, amidst increasing demands for transparency and accuracy. As these systems integrate into business operations, understanding their effectiveness in mitigating risks and ensuring compliance with GAAP is essential for maintaining financial integrity and stakeholder confidence. This study aims to assess and understand the extent of the effectiveness of the audit application information system in providing accurate and timely information, as well as reducing risks within acceptable limits by the company. An examiner has the principal intention to provide an opinion on the feasibility of financial statements in all significant aspects in accordance with Generally Accepted Accounting Principles (PABU). The point is to ensure that users of financial statements have confidence that the report has been prepared in accordance with established standards, and therefore, evaluation from third parties that are free from related interests is needed. The approach used is a descriptive approach based on quantitative analysis by collecting data from various articles and websites used as references. In application audits, it is also common to check general controls because general controls contribute to the effectiveness of application controls.

Keywords: *Audit, Information System Audit, Audit Concept*

1. INTRODUCTION

In this modern era, the development of the business world takes place rapidly and continues to develop, causing complexity of problems for business entities. In such situations, there is the potential for errors in the presentation of financial statements. Therefore, the role of auditors in the business world has great significance. Auditor is a professional expert whose duty is to audit the financial statements of an entity and conclude the appropriateness of the financial statements. With this audit, stakeholders can trust the audited financial statements and make the right decisions.

Examination in information systems is a significant process in maintaining the integrity, security, results, and productivity of an entity's information system. In the ever-evolving digital era, information systems are the cornerstone of fundamental business operations, making it crucial to ensure that the system functions smoothly and in accordance with established provisions. Information systems audits involve collecting and evaluating evidence to determine whether the computer systems used have been able to protect the assets owned by the entity, maintain data integrity, make an effective contribution to the achievement of the entity's objectives, and use resources efficiently. Information systems auditors are responsible for conducting a thorough examination of the information system and making conclusions regarding the appropriateness of financial statements and the reliability of the application system.

In this study, the concept and application of auditing in information systems will be discussed. First, the basic concepts of information system auditing will be explained, including the objectives and principles of auditing and the role of auditors in maintaining the reliability of information systems. Furthermore, the application of auditing in information systems will be discussed, including audit techniques and methods used, risk assessment, internal control, and quality assessment of information system management and development. Business risk assessment conducted by auditors is the first step in audit planning to conduct audit testing and collect evidence (Qothrunnada, 2022). Auditors need adequate and relevant evidence. By conducting an accurate business risk assessment, auditors can determine the scope and scope of audit evidence collection. Since in the performance of audit duties, the auditor does not thoroughly examine all audit evidence, sampling is a common procedure used by auditors. Therefore, auditors are expected to use their professional judgment in the audit process to prevent failures. The auditor's ability to make appropriate judgments in their audit duties reflects their professionalism.

Through a deep understanding of the concept and application of auditing in information systems, it is expected that readers can understand the importance of information system audits in maintaining the integrity and reliability of information systems, as well as being able to apply audit principles to ensure the effectiveness and efficiency of information system management in organizations.

The novelty of this research lies in the innovative approach that combines risk-based auditing and control-based auditing in the evaluation of information systems. This research not only focuses on identifying the risks that exist in information systems, but also evaluates the effectiveness of the controls implemented to manage these risks. This approach allows organizations to get a more holistic picture of the security, integrity, availability, and compliance of their information systems. In addition, this research makes a significant contribution by offering a more integrative framework, which can assist organizations in improving the overall reliability and security of their information systems. Thus, this research provides a new in-depth and practical outlook for the application of information systems auditing in various organizations.

2. LITERATURE REVIEW

2.1. Audit Definition

Auditing is a systematic and independent process for examining, evaluating, and verifying the information, records, transactions, and procedures of a business entity or organization (Zamzami et al., 2018). The purpose of an audit is to determine the appropriateness, reliability, and validity of the financial information presented in an entity's financial statements. The auditor, who is usually an independent third party, conducts evidence gathering, analysis, and assessment of the entity's systems, policies, and business practices to ensure that the financial statements are prepared in accordance with applicable accounting standards and relevant financial principles. Audit results are submitted in the form of an auditor's report expressing an opinion on the appropriateness of the audited financial statements. Audits help improve the trust and reliability of financial information, protect the interests of stakeholders, and provide users with

confidence that they reflect their actual financial condition and comply with applicable regulations and requirements (Rahmanto et al., 2020).

The audit process involves steps such as audit planning, evidence collection and analysis, risk assessment, internal control testing, and substantive testing (Herawati, 2008; Wadiyo, 2024). Auditors follow established audit standards, such as Audit Standards issued by the governing body of the accounting profession. During the audit process, auditors must maintain independence, objectivity, and integrity in carrying out their duties.

Audits can be conducted by internal auditors who are part of the business entity itself, or by external auditors who are independent parties not related to the entity. External auditors generally hold professional certifications, such as Chartered Accountant (CA) or Certified Public Accountant (CPA), which provide legitimacy and confidence in their qualifications and competence in conducting audits. By conducting regular audits, business entities can ensure regulatory compliance, improve operational efficiency, identify areas of improvement, and strengthen trust from stakeholders such as shareholders, lenders, and investors.

2.2. Audit Objectives

The objectives of the audit in general can be classified as follows:

a. Completeness. To verify that all transactions have been recorded completely and nothing has been missed.
b. Accuracy. To ensure that transactions and forecast balances recorded have the right amount, correct calculations, proper classification, and accurate record-keeping.
c. Existence. To verify that all recorded assets and liabilities actually existed or occurred on a particular date, so that the recorded transactions are real transactions and not fictitious.
d. Valuation. To ensure that generally accepted accounting principles have been correctly applied in the valuation of assets, liabilities, and other elements of financial statements.
e. Classification. To ensure that recorded transactions have been correctly classified in the journal. If it is related to the balance, the figures listed in the client's financial statements must be classified appropriately.
f. Accurate (Accuracy). To verify that all transactions were recorded on the correct date, the details in the account balance correspond to the general ledger records, and the summation of the balance has been made appropriately.
g. Cut-off. To ensure that transactions that occur close to the balance sheet date have been recorded in the appropriate period. Transactions that may have a risk of misstatement are those that are recorded towards the end of the accounting period.
h. Disclosure. To verify that account balances and relevant disclosure requirements have been clearly presented in the financial statements and adequately described in the contents and footnotes of such reports**.**

2.3. Audit Benefits

The existence of audit checks plays a role in increasing the authenticity of financial statements that can be trusted by external parties such as shareholders, creditors, government authorities, and so on. In addition, audits can prevent fraudulent actions

committed by the management of the company being audited. Audits provide significant benefits, here are some of them:

a) Verification and Validation: Audits help verify and validate the correctness, accuracy, and completeness of financial information contained in financial statements. This provides confidence to stakeholders that the financial statements are in accordance with applicable accounting principles and reflect the actual financial condition.
b) Fraud and Abuse Detection: Auditing involves examining a company's internal systems, policies, and procedures to detect potential fraud, abuse, or violations of the law. Thus, audits can uncover unethical or illegal practices, helping to protect companies from adverse financial and reputational losses.
c) Increased Efficiency and Effectiveness: Through the audit process, auditors provide recommendations to improve the efficiency and effectiveness of the company's operations. This includes identifying weaknesses in systems, internal controls, and business procedures, as well as providing suggestions for improvements that can improve the company's productivity and performance.
d) Stakeholder Trust and Satisfaction: Independent and objective audits provide confidence to stakeholders that the company's financial statements have been carefully and can be trusted. This increases the trust, satisfaction, and loyalty of shareholders, creditors, investors, and other related parties.
e) Regulatory and Standard Compliance: Audits ensure that the company complies with applicable regulations, laws, and accounting standards. This helps protect the company from sanctions and legal risks, as well as strengthens the company's reputation as an entity that operates with integrity and in accordance with established requirements.
f) Risk Evaluation and Control: Auditors help in identifying and evaluating the risks faced by the company. By analyzing internal controls and business processes, auditing helps in risk control and better decision making in managing the risks associated with the company's operations.

2.4. Types of audits

Based on the domain of the audit conducted, there are six types of audits that can be carried out. First, Financial Audit is used to thoroughly evaluate the conformity of financial statements with predetermined criteria (NISP, 2023). Second, Operational Audit aims to test effectiveness, efficiency, and economics in a specific field of activity. Furthermore, a Compliance Audit is conducted to verify the client's or customer's compliance with procedures or regulations set by the authorities. An e-commerce audit focuses on examining business activities related to e- commerce, including disclosure of business practices, trust in transaction reliability, and information protection. Fraud Audit refers to an examination of fraudulent acts involving management in manipulating financial statements or assets and profits with the intention of deceiving parties outside the organization. Finally, Information Systems Audit is the process of collecting and evaluating evidence to assess whether the computer systems used protect organizational

assets, maintain data integrity, help achieve organizational goals effectively, and use resources efficiently.

3. RESEARCH METHODS

In this research, the method used was qualitative description sourced from relevant information accompanied by inductive data analysis. This approach was carried out systematically and clearly structured to ensure accuracy and regularity in data collection and analysis. The types and sources of data used in this research were indirect data, which were obtained from various examples of articles and various websites on the internet that were used as references. By relying on these secondary sources, the research explored and interpreted existing information to provide a comprehensive and in-depth picture of the topic under study.

4. RESULTS AND DISCUSSION

The concept of audit in information systems plays a crucial role in maintaining the security and integrity of the system. Audit involves a systematic examination of records and activities within an organization to ensure accuracy, completeness, and compliance with relevant policies and regulations. This process is essential for identifying vulnerabilities, detecting and preventing harmful activities, and ensuring the functioning of security controls. Several key aspects determine the implementation of audits in information systems. First, audits ensure proper access controls by monitoring user logins, permissions, and actions within the system. Second, audits help identify security threats and vulnerabilities through monitoring system logs and network traffic, enabling proactive measures to reduce risks. Third, audits ensure compliance with laws, regulations, and industry standards, verifying the implementation and effectiveness of security controls and data backup procedures. Additionally, audits contribute to risk management by identifying and assessing potential risks in information systems and enabling actions to minimize their impact. Furthermore, routine monitoring and testing of security controls and system logs allow real-time detection and response to security incidents. Lastly, audits provide detailed reporting and analysis of system activities, aiding in the identification of trends, patterns, and security issues to enhance controls and prevent future incidents. In essence, the concept and implementation of audits in information systems are crucial for maintaining security, integrity, and compliance with regulations and standards.

4.1. Information System Audit

An information system audit is a process carried out to evaluate the reliability, security, efficiency, and effectiveness of information systems in an organization (Gondodiyoto, 2007; I Putu Agus Swastika et al., 2016). This audit aims to ensure that computer systems and processes related to information management run properly and in accordance with applicable policies, standards, and regulations.

Information systems examination involves the process of collecting and evaluating evidence to determine whether the computer system used has successfully protected organizational assets, maintained data integrity, supported the achievement of

organizational goals effectively, and utilized resources efficiently (Pratiwi, 2021). This definition is in line with the objectives of Internal Quality Inspection in ISO 9001:2000. The Information Systems Examination combines various fields of science, including Traditional Examination, Information Systems Management, Accounting Information Systems, Computer Science, and Behavioral Science (Wunady, 2024).

Broadly speaking, Information System Audit can be divided into two categories, namely Application Control and General Control. General Control aims to maintain the integrity of data in computer systems and ensure the integrity of programs or applications used in data processing. Meanwhile, Application Control aims to verify the correctness of data input into the application, ensure accurate data processing, and provide adequate control of the output results.

Information Systems Examination is the process of acquiring and evaluating evidence to assess whether the use of computer systems has succeeded in protecting organizational assets, maintaining data integrity, supporting the achievement of organizational goals effectively, and utilizing resources efficiently. This check involves application control and general control. General control aims to maintain the integrity of data in the computer system and verify the integrity of the program or application used. On the other hand, application control aims to verify that data is inputted with accuracy, processed appropriately, and there is adequate control over the results produced.

4.2. Application of Audit in Information Systems

Application control relates to the controls applied in the application or program used to process data The purpose of application control is to verify the accuracy of data input into the application, ensure proper data processing, and provide adequate control over the resulting output (Sukmajaya & Andry, 2017). This involves checking the accuracy, correctness, and validity of the data entered into the system. In addition, application control also includes testing data validity, verifying the feasibility of processing, and handling and securing the resulting output.

An audit of applications and information systems involves an examination of the control and reliability of applications used in data processing, as well as an evaluation of the overall infrastructure and processes of information systems used by the organization. This audit aims to ensure that the data is inputted correctly, processed accurately, and the output produced is reliable. In addition, the audit also focuses on the protection of organizational assets, system security, data integrity, and infrastructure availability and reliability. The results of the information system audit provide insight into the weaknesses and strengths of the system, so as to provide recommendations for improvement and development to improve the quality and efficiency of the information system.

4.3. Purpose of Information System Audit

As an instrument, this information system requires inspection. In order to ensure the quality of the information system. The objectives of information system audit can be generally summarized into 5 stages, namely:

a) Increase the security of company assets
   Company information assets such as hardware, software, human resources, and data files must be maintained by a good internal control system so that asset misuse does

not occur.

b) Improve and maintain data integrity
Data integrity is the basic principle of information systems. Data must have attributes such as completeness, correctness, and accuracy. Without keeping data intact, organizations cannot properly reflect the situation.

c) Increase system effectiveness
The effectiveness of corporate information systems is very important in decision making. Information systems are said to be effective if they are in accordance with user needs.

d) Increase system efficiency
System efficiency is important by considering adequate capacity. When the computer no longer has

e) Economy
Economics reflects cost/benefit calculations that focus more on monetary value. In addition, the objectives of information system audit can be grouped into two main aspects in information technology management, namely:

f) *Conformance* - In this category of objectives, information systems audits are focused on determining compliance, such as confidentiality, integrity, availability, and compliance.

g) Performance - In this category of objectives, information systems audits are focused on evaluating performance, such as effectiveness, efficiency, and reliability.

4.4. Risk-Based Information System Audit

Risk-based information systems auditing is an approach used to identify and evaluate the risks associated with an organization's information systems. In this audit, the first step is to identify potential risks that could affect information systems, such as security threats, human error, or system failure. Furthermore, a risk evaluation is carried out to assess the extent to which these risks can affect the organization's systems and operations. Based on the risk evaluation, the audit plans an appropriate approach, including the setting of audit objectives, scope, and audit methods. During the audit, tests are carried out on the controls that have been implemented in the system to evaluate their effectiveness. The results of these audits provide insight into the risks present and assist the organization in taking action to mitigate the risks and improve the security and performance of information systems.

In a risk-based information system audit, testing of existing controls in the system is carried out. This test aims to evaluate the effectiveness of controls that have been implemented in managing these risks. For example, testing can be performed to ensure that access control to systems is only provided to authorized users, or to verify that disaster recovery measures have been properly planned and implemented.

In addition, risk-based information system audits also involve an assessment of compliance with applicable policies and regulations. The auditor will check whether the information system has complied with data security and privacy standards regulated by industry laws or regulations. This is important to ensure that the organization complies with applicable legal requirements and protects the interests of data users and related parties.

The results of a risk-based information systems audit provide valuable information to the management and stakeholders of the organization. The auditor will provide recommendations to improve weaknesses found in the information system, reduce existing risks, and improve the effectiveness and security of the system as a whole. Thus, risk-based information system audits assist organizations in managing risks related to information systems, maintaining compliance, and improving information system performance and security.

4.5. Control-Based Information System Audit

In carrying out their duties, information systems auditors gather adequate evidence through a variety of methods including surveys, interviews, observations, and document reviews (including source code reviews if necessary). Interestingly, evidence collected by auditors generally involves electronic evidence (information in the form of digital files). In general, information systems auditors utilize computer-aided auditing methods, also known as CAAT (Computer Aided Auditing Technique). This approach is used to analyze information, such as data including sales, purchases, inventory, customer activity, and others. According to ISACA (Information Systems Audit and Control Association) guidelines, in addition to performing field tasks, auditors also need to compile reports that include the purpose of the audit, the level of detail of the audit performed, and the characteristics of the audit carried out. The report must also include the name of the organization being examined, the party to which the report is addressed, and restrictions on distribution of the report. The report also needs to include findings, conclusions, and recommendations like audit reports in general. Control can reduce the risk of unwanted errors by reducing the probability of undesirable events occurring and limiting the impact of errors if they occur. In a control-focused audit, a series of activities are carried out to evaluate the reliability of existing controls, referring to the ISO 9001-2000 quality management standard.

4.6. Control-Based Information System Audit

In line with the increasing use of computers in supporting company operations, it is essential to have appropriate guidelines as internal control tools to ensure that electronic data processed has a high level of accuracy. The purpose of this is so that the electronic data can produce reliable company financial statements. In its development, there have been many control guides that have emerged as a result of various diverse backgrounds. Therefore, in this explanation will be described several types of EDP control guidelines, such as the Committee of Organizations of Persons (COSO), COBIT, SARBOX, ISO 17799, and BASEL II.

Control-based information system audit is an approach taken to evaluate the effectiveness and reliability of controls implemented in an organization's information systems. The purpose of this audit is to ensure that existing controls can prevent, detect, and address risks associated with information systems.

In a control-based information system audit, the auditor will check the existence and effectiveness of controls that have been implemented in the system. These controls include aspects of security, integrity, availability, and compliance with applicable policies

and regulations. The auditor will test these controls to evaluate whether they are functioning as expected.

In addition, the auditor will also evaluate the reliability of the control management process carried out by the organization. This includes an assessment of established monitoring policies, procedures, and actions to ensure that controls remain effective and appropriate to the needs of the organization. The auditor will prepare an audit report that includes findings, improvement recommendations, and conclusions related to the reliability of the information system and existing controls.

By conducting a control-based information systems audit, organizations can gain deep insight into the reliability and effectiveness of the controls implemented in their information systems. These audits assist organizations in identifying and remediating existing weaknesses, improving system security and performance, and ensuring that relevant policies and regulations are adhered to.

Audits play an important role in detecting information system vulnerabilities by utilizing various methods and tools. The utilization of audit application information systems plays an important role in improving the efficiency, accuracy, and consistency of the audit process within the company. These systems enable automation, accurate data collection, quick analysis, and efficient report generation, ultimately providing accurate and timely information (Wahono et al., 2023). In addition, effective implementation of information systems audits has a positive impact on internal control, improving the quality of internal supervision and transparency (Xu, 2020). Overall, the integration of audit application information systems not only optimizes resource allocation and reduces management costs but also improves the quality of audit reports and procedures, ultimately reducing risks within acceptable limits (Almasria et al., 2021; Sayed, 2019). The utilization of audit application information systems plays an important role in improving the efficiency, accuracy, and consistency of the audit process within the company. These systems enable automation, accurate data collection, quick analysis, and efficient report generation, ultimately providing accurate and timely information (Wahono et al., 2023). In addition, effective implementation of information systems audits has a positive impact on internal control, improving the quality of internal supervision and transparency (Xu, 2020). Overall, the integration of audit application information systems not only optimizes resource allocation and reduces management costs but also improves the quality of audit reports and procedures, ultimately reducing risks within acceptable limits (Almasria et al., 2021; Sayed, 2019). Open source intelligence (OSINT) techniques extend conventional auditing capabilities by uncovering hidden information from restricted access within an organization's information resources, such as non-indexed files containing sensitive data or proprietary technology (Melshiyan & Dushkin, 2022). Security audits, such as those conducted using the OWASP ZAP tool, help to identify and address vulnerabilities that can be exploited by attackers, ensuring system security (Melshiyan & Dushkin, 2022). Penetration tests, such as gray box testing, are instrumental in identifying high, medium, and low vulnerability categories in information systems, enabling targeted security enhancements to protect critical data and infrastructure (Pirsa & Sumijan, 2020). By performing network scans and using descriptive research methodologies, audits can pinpoint vulnerabilities in systems like Finanzas al Día S.A.S, enabling proactive mitigation to prevent unauthorized access and data breaches (Ramírez et al., 2022).

Information system examination is the process of collecting and assessing evidence to check whether the use of computer systems has been able to protect company assets, maintain data integrity, support the achievement of organizational goals effectively, and utilize resources with efficiency. The purpose of an information systems audit, as argued, can be summed up into five main stages. First, it increases the security of company assets. Second, improve and maintain data integrity. Third, increase the effectiveness of the system. Fourth, improve system efficiency. And fifth, consider the economic aspect. In an information systems audit, the auditor will collect and evaluate evidence to assess the extent to which the computer system has met these objectives. This includes reviewing security controls in place to protect company assets, checking the reliability and integrity of data processed, and evaluating the effectiveness and efficiency of resource use in the system. This audit also considers the economic aspect, namely the cost-benefit calculation of the controls applied.

After reviewing the Information System Audit, we will have an understanding of the concept of information system / information technology audit, the associated risks, the controls recommended to be applied, as well as an examination of the quality of information system management, system application development, and the reliability of certain application systems. This check can be performed either manually or by using computer-aided auditing techniques.

The practical implication of this research is that organizations can adopt a more holistic and integrative audit framework, which incorporates both risk- and control-based approaches to improve the reliability and security of their information systems. By identifying risks and evaluating the effectiveness of existing controls, organizations can strengthen risk mitigation strategies and ensure compliance with applicable regulations. In addition, the findings of this study can assist management in making more informed and strategic decisions regarding investments in the security and management of information systems. Theoretically, this research contributes to the information systems audit literature by offering a new perspective on the integration of risk- and control-based approaches. It expands the understanding of how these two approaches can be used synergistically to achieve more comprehensive and effective audit results. This research also opens up opportunities for follow-up studies to test and validate the proposed framework in a variety of different organizational and industry contexts.

5. CONCLUSION

The conclusion from the results of this study shows that the implementation of information systems auditing with an approach that combines risk-based auditing and control-based auditing provides significant benefits to organizations. Through risk-based auditing, organizations can identify and evaluate the risks that might affect their information systems, thus enabling them to take appropriate preventive measures. Meanwhile, control-based audits focus on assessing the effectiveness of the controls implemented to manage those risks, including aspects of security, integrity, availability, and compliance.

The research also emphasizes that by integrating these two approaches, organizations can gain a more holistic and comprehensive picture of the condition and

performance of their information systems. Audit results provide valuable insights that can be used to improve the security and reliability of information systems, as well as ensure compliance with applicable regulations. Overall, this research underscores the importance of combining risk- and control-based auditing as an effective framework for evaluating and improving an organization's information systems.

REFERENCES

Almasria, N., Airout, R. M., Samara, A. I., Saadat, M., & Jrairah, T. S. (2021). The role of accounting information systems in enhancing the quality of external audit procedures. *Journal of Management Information and Decision Sciences*, *24*(7), 1–23.

Gondodiyoto, S. (2007). Information System Audit+ Approach of COBIT. *Jakarta: Mitra Wacana Media*.

Herawati, E. (2008). Audit Sistem Informasi Aplikasi Persediaan Pada PT SS. *ComIT*, 95–98.

I Putu Agus Swastika, M. K., I Gusti Lanang Agung Raditya Putra, S. P. M. T., Pramesta, A., OFFSET, C. V. A., & Primakara, S. (2016). *Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus*. Penerbit Andi.

Melshiyan, M. A., & Dushkin, A. V. (2022). Information Security Audit Using Open Source Intelligence Methods. *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, 379–382.

Pirsa, N., & Sumijan, S. (2020). Meningkatkan Keamanan Sistem Informasi Puskesmas Terpadu dengan Metode Grey-Box Penetration Test Menggunakan Computer Assisted Audit Techniques. *Jurnal Informasi Dan Teknologi*, 133–138.

Pratiwi, F. (2021). *Audit Sistem Informasi, Kenali Apa Itu, Tujuan dan Tahapannya*. Harmony.

Qothrunnada, K. (2022). *Bisnis: Pengertian, Tujuan, Jenis dan Contohnya*. Detikfinance.

Rahmanto, Y., Ulum, F., & Priyopradono, B. (2020). Aplikasi pembelajaran audit sistem informasi dan tata kelola teknologi informasi berbasis Mobile. *Jurnal Tekno Kompak*, *14*(2), 62–67.

Ramírez, S. S., Londoño, Á. M., Barco, Y. A. Q., Villa, C. F. H., & Ramírez, F. D. J. C. (2022). Desarrollo de un sistema de seguridad informática a partir de una auditoría sobre una red empresarial. *INGENIERÍA: Ciencia, Tecnología e Innovación*, *9*(2), 135–151.

Sayed, T. A. (2019). The Effectiveness of Accounting Information Systems in Reducing the Risks of Electronic Auditing: Applied Study on Irbid's Electricity Company of Jordan. *International Journal of Business and Management*, *14*(4), 205–2015.

Sukmajaya, I. B., & Andry, J. F. (2017). Audit Sistem Informasi pada Aplikasi Accurate Menggunakan Model Cobit Framework 4.1 (Studi Kasus: PT. Setia Jaya Teknologi). *Seminar Nasional Teknoka*, *2*, 45–54.

Wadiyo, S. E. (2024). *Mengenal Lebih Dekat Internal Audit: Konsep, Tujuan, dan Struktur Organisasi*.

Wahono, P. S., Safuan, S., & Alhabshy, M. A. (2023). Penggunaan Aplikasi E-Audit Dalam Sistem Informasi Manajemen Inspektorat Polri. *Jurnal Ilmiah Global*

Education, *4*(2), 1122–1130.

Wunady, J. (2024). *Apa Itu Audit Sistem Informasi? Pengertian, Tujuan dan Manfaatnya*. Maserp.

Xu, B. (2020). Analysis of the Application of Information System in Financial Management Auditing. *Cyber Security Intelligence and Analytics: Proceedings of the 2020 International Conference on Cyber Security Intelligence and Analytics (CSIA 2020), Volume 2*, 243–248.

Zamzami, F., Faiz, I. A., Press, U. G. M., Press, G. M. U., Riadi, M., I Putu Agus Swastika, M. K., I Gusti Lanang Agung Raditya Putra, S. P. M. T., Pramesta, A., OFFSET, C. V. A., & Primakara, S. (2018). *Definition, Indicators and Measurement of Audit Quality*. Penerbit Andi.

Copyrights