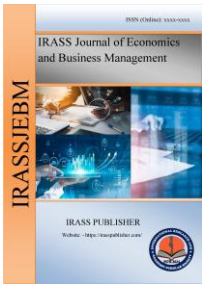
IRASS Journal of Economics and Business Management
Abbriviate Title- IRASS J Econ Bus Manag
ISSN *(Online) 3049-1320*
https://irasspublisher.com/journal-details/IRASSJEBM
Vol-1, Iss-1(December-2024)



Information Technology Audit in the Midst of the Digital Revolution: Integrating Risk Management, Control, and Regulatory Compliance

Nada Cuary[1*], Siti Maharani Diandra[2], Iskandar Muda[3], Gusnardi[4]

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

[4] Universitas Riau, Pekanbaru, Indonesia

Corresponding Author Nada Cuary

Universitas Sumatera Utara, Medan, Indonesia

Article History

Received: 23 / 11/ 2024

Accepted: 11 / 11 / 2024

Published: 14 / 12 / 2024

Abstract: Information Technology (IT) Audit is an important element in maintaining the security and effectiveness of information systems in modern businesses that increasingly rely on technology. With the implementation of new technologies such as cloud computing, Mobile Device Management (MDM), and the Internet of Things (IoT), the need for effective IT audits is increasingly urgent to identify and mitigate risks. The study highlights the role of IT audits in ensuring compliance with data privacy regulations, such as GDPR, as well as in building organizational awareness of data protection. The findings show that while technologies like ERP offer efficiency, proper controls are indispensable to protecting information assets. With a proactive approach, IT auditors can provide recommendations for improving systems and support organizations in creating a strong data protection culture.

Keywords: IT Audit, Information Technology, Risk, Compliance, Data Protection, Cloud Computing, GDPR..

1. Introduction

1.1 Background

Information Technology (IT) has become an integral component of modern business operations. In today's digital era, almost all business sectors rely on information systems to manage data, improve operational efficiency, and support strategic decision-making. As the use of IT in various fields increases, the need for effective control and auditing of IT systems is increasing (Pu et al., 2024). Strong controls are needed to ensure that IT systems function efficiently, safely, and in accordance with the organization's strategic goals. Basically, IT audits play an importantrole in evaluating the reliability, integrity, and security of information generated by IT systems, especially highly sensitive financial information (Agung Wijoyo, 2023).

IT auditors are responsible for ensuring that the controls implemented by the organization are adequate in protecting information assets. They must ensure that the system used is able to run well and is aligned with the organization's strategic goals. However, an IT audit does not only cover the technical aspects of information systems (Rajesh et al., 2022). Conversely, IT audits should also include compliance with relevant regulations, privacy policies, and risk management. The development and maintenance of secure, compliant, and efficient information systems is a top priority in a world that is increasingly dependent on technology (Farah Ashama, 2024).

Along with the rapid development of technology, changes in the IT environment such as the adoption of cloud computing, mobile device management (MDM), and the Internet of Things (IoT) are becoming new challenges for auditors. In this context, auditors are required to deeply understand how these technologies work and how appropriate controls can be applied to address the risks that arise. The application of cloud computing, for example, allows companies to store and access data remotely via the internet. However, this implementation also opens up new opportunities for risks such as unauthorized access, data leaks, and greater security vulnerabilities compared to traditional systems. Likewise, the implementation of MDM, which facilitates the use of mobile devices for work purposes. However, it also increases the company's information security risks, especially if the device is used for employees' personal purposes.

In addition, IoT connecting various devices over the internet has revolutionized the way businesses operate. For example, the use of sensors and smart devices in production, logistics, and asset management provides companies with real-time access to the data needed for strategic decision-making (Khan et al., 2023). However, keep in mind that the more devices are connected, the greater the potential risk to data and system security.

One of the key technologies that is currently widely used in business management is Enterprise Resource Planning (ERP). ERP is a software system that provides standard business functionality in one integrated IT system. This system allows various organizational functions, such as human resource management, finance, production, and supply chain, to share information from the same database. This not only reduces storage costs, but also

© Copyright IRASS Publisher. All Rights Reserved

improves the consistency and accuracy of data from the same source.

However, like any other technology, ERP implementation is not free from risks. Some of the risks that are often faced by organizations implementing ERP include modifications required to accommodate organization-specific business processes, reliance on a single vendor for technical support, as well as security risks associated with access to a single database. Therefore, it is important for IT auditors to thoroughly evaluate the implementation and controls in ERP systems, to ensure that they function effectively and securely.

In a dynamic IT environment, the importance of risk management in IT audits cannot be overlooked. Evolving technologies create new risks that must be identified, evaluated, and properly managed. Risk management is a critical process that allows organizations to identify potential threats to IT systems and develop appropriate mitigation measures to protect those systems from such threats. The risks faced by information systems can come from a variety of sources, including cyberattacks, human error, and system failures. Therefore, organizations must implement a comprehensive risk management strategy, which includes risk identification, impact analysis, vulnerability assessment, and the establishment of appropriate mitigation measures. IT auditors play an important role in ensuring that the organization has implemented effective controls to manage these risks. One of the tools used in this process is Computer- Assisted Audit Techniques (CAATs). This technique allows auditors to use computer-aided tools to analyze data and identify potential problems in IT systems. By using CAATs, auditors can improve the effectiveness and efficiency of the audit process, as well as identify potential risks that may have been missed in manual audits (Nasution et al., 2022).

In addition to risk management, IT audits should also pay attention to compliance with regulations and privacy policies. Along with growing concerns about data privacy, governments around the world have enacted various laws and regulations governing the management of personal data. IT auditors must ensure that the information systems used by organizations comply with all relevant regulations, such as the General Data Protection Regulation (GDPR) in the European Union, which governs how personal data should be collected, stored, and used. Additionally, an organization's privacy policy should be designed to protect sensitive customer and employee information from unauthorized access. IT auditors

are responsible for ensuring that such privacy policies are implemented consistently across the organization, and that there are adequate oversight mechanisms in place to detect and address privacy breaches (Ida Agustin 2024).

Information Technology (IT) audits have a strategic role in ensuring that an organization's information systems function effectively, safely, and comply with all applicable regulations. In an increasingly technology-dependent world, IT auditors must not only understand the technical aspects of information systems, but also have in-depth knowledge of regulations, privacy policies, and risk management. The use of modern technologies such as cloud computing, MDM, and IoT has opened up new opportunities for businesses, but also created new challenges that auditors must face. Effective risk management, the implementation of appropriate controls, and compliance with privacy regulations are key elements in an IT audit. By using computer-aided auditing techniques (CAATs), auditors can improve the efficiency of the audit process and ensure that an organization's information systems are protected from existing threats. In the future, the role of IT auditing will continue to evolve as technology changes, and IT auditors must always be prepared for new challenges that may arise.

2. Literature Review

In the literature written by Otero (2018) in Information Technology Control and Audit, it is stated that Information Technology (IT) audits play an important role in ensuring the effectiveness of information system control and security in modern organizations. This review is in line with previous research that has shown how IT controls and audits are key elements in mitigating risks and improving regulatory compliance. Here are some related studies that reinforce and expand the concept outlined by Otero.

Research by Kuhn and Sutton (2010) discusses the importance of implementing controls in information systems, which is in line with Otero's view of controls in IT audits. They emphasized that risks in IT can have a significant impact on the integrity and accuracy of an organization's data. This study shows that strong controls, both at the infrastructure and application level, are critical to preventing internal and external threats. Otero (2018) also corroborates this by emphasizing the importance of audits that focus on controls, both in traditional IT systems and the latest technologies such as cloud computing and Mobile Device Management (MDM).

Another relevant research is the work by Hunton, Bryant, and Bagranoff (2004), which emphasizes the need for audits of information systems to prevent and detect potential errors and fraud. This study reinforces Otero's argument about the importance of computer-assisted audit techniques (CAATs). With the rapid development of technology, CAATs have proven to assist auditors in analyzing large amounts of data more quickly and effectively, a key point outlined in Otero's book.

IT risk management is also a major concern in the IT audit literature. Research conducted by Gordon, Loeb, and Sohail (2010) shows that proper IT risk management contributes to organizational performance by helping organizations recognize and respond to possible threats. This research is in line with Otero's (2018) view of how risk management should be an integral part of the IT audit process. The study identifies the risks associated with the adoption of technologies such as cloud computing and IoT, as well as how organizations can leverage IT audits to minimize potential losses.

Meanwhile, research by Rainer, Snyder, and Carr (1991) examined the risks in the management of information systems and found that these risks are often overlooked, especially in the adoption of new technologies. This underscores the importance of a deep understanding

of technology by auditors, which was also a key theme in Otero's discussion on the need for auditors to understand technologies such as ERP, cloud computing, and MDM. This research reinforces Otero's argument that in-depth knowledge of technology is essential to ensure that auditors can effectively identify and mitigate risks.

© Copyright IRASS Publisher. All Rights Reserved

Research on regulatory compliance related to data privacy has also been the focus of several previous studies. For example, research conducted by Smith, Dinev, and Xu (2011) highlights the importance of compliance with privacy regulations, especially with growing concerns about the handling of personal data. The study emphasizes that organizations must proactively manage personal data and ensure compliance with laws such as GDPR. Otero (2018) also emphasizes the importance of compliance with privacy and security regulations, especially in the context of IT, as well as the importance of controls to ensure an organization's data is protected from unauthorized access.

In addition, research by Kroll, Barocas, and Felten (2017) shows that privacy violations can have a serious impact on a company's reputation and operations. This research supports Otero's argument about the need for IT audits to ensure that organizations comply with applicable information security standards, such as COBIT and ISO/IEC 27002. Strengthening these regulations, both nationally and internationally, has become a key focus in IT audits to protect organizations from regulatory and reputational risks.

Previous studies have clearly demonstrated the importance of audits and controls in managing risk and information security in IT systems. Studies by Kuhn and Sutton (2010), Hunton et al. (2004), and Gordon et al. (2010) are in line with the findings of Otero (2018) which states that appropriate controls and computer-aided audits (CAATs) play an important role in risk mitigation. In addition, research on regulatory compliance by Smith et al. (2011) and Kroll et al. (2017) also corroborates Otero's view of the importance of compliance in IT audits to protect data privacy and organizational reputation. As such, the existing literature supports and expands on the argument that IT audits play a crucial role in maintaining the security, efficiency, and compliance of information systems in modern organizations.

3. Writing Method

This paper is prepared using analytical descriptive methods, with the main focus on literature review and comparative analysis. Descriptive analytic according to Sugiyono (2013:206), is a method that functions to describe or provide an overview of an object that is being researched through data or samples that have been collected as it is without conducting analysis to make conclusions that apply to the public. This method was chosen to explore a deeper understanding of the importance of Information Technology (IT) audits as well as effective controls in ensuring the security, integrity, and compliance of an organization's information systems. In preparing this paper, the author incorporates the following steps:

3.1 Collection of Related Literature

The Initial stage in the writing of this paper is the collection of literature from various academic and practical sources relevant to the theme of IT audit. The main sources used in this paper include Angel R. Otero's book Information Technology Control and Audit (2018), related academic journals, and previous research reports that address similar themes. Otero's book is used as the main basis because it presents the latest concepts regarding IT auditing, information systems control, risk management, and regulatory compliance. This process involves identifying relevant literature from academic databases such as Google Scholar, JSTOR, ProQuest, and e-book portals. Keywords used in the search include "IT audit," "information systems control," "IT risk management," "CAATs," "cloud computing," "data privacy compliance," and "Enterprise Resource Planning (ERP)." This literacy helps in building a strong theoretical framework and provides a comprehensive basis for further analysis.

3.2 Literature Review

After the literature collection, the next stage is to conduct an in-depth study of the collected materials. The collected literature is carefully read and analyzed to understand the key themes related to IT audits. This literature review is used to provide a basis for discussion on various aspects of IT control and the role of auditors in ensuring security and regulatory compliance. The literature analysis focuses on identifying the key risks associated with IT systems, the benefits of implementing effective controls, and auditing techniques that can be used by auditors to improve audit accuracy and efficiency. Additionally, literature reviews also provide insights into the latest developments in technologies, such as cloud computing, IoT, and Mobile Device Management (MDM), which are changing the IT audit landscape.

3.3 Comparative Analysis

One of the main methods used in this paper is comparative analysis, where previous research is compared with the findings and concepts outlined by Otero (2018). This analysis focuses on looking for suitability, differences, and contributions from previous research to the development of modern IT auditing practices. Some of the research used as a reference includes research by Kuhn and Sutton (2010), Hunton et al. (2004), and Smith et al. (2011), which discuss IT controls, computer-aided auditing techniques (CAATs), and regulatory compliance. By using this method, the author is able to see how the concepts discussed in the book Otero (2018) are in accordance with or different from previous views. This helps provide a richer understanding of how IT audits are evolving and the challenges faced by auditors in ensuring the effectiveness of controls amid an ever-changing technology environment.

3.4 Writing and Drafting

After the literature review and analysis is complete, the author compiles and organizes the relevant information into a coherent narrative form. The writing structure begins with an introduction, followed by a literature review, methodology, analysis, and conclusion. Each section is designed to discuss a specific topic in detail and logically, with the goal of providing readers with a comprehensive understanding of the importance of IT audits. The introduction section provides background on the importance of IT audits and the role of controls in maintaining data security and integrity. A literature review traces the development of IT audit theory, while the analysis provides deeper insights into how these concepts are applied in practice. The conclusions summarize the main findings of this review and provide recommendations for further development in IT audits.

By following the above methods, the author seeks to present a paper that is not only descriptive but also provides an in-depth analysis related to Information Technology (IT) audits. Through a descriptive approach, the author describes the developments and challenges faced by IT auditors in the face of ever-evolving technological advancements, such as the adoption of cloud computing, Mobile Device Management (MDM), and the Internet of Things (IoT). Meanwhile, an analytical approach is used to

© Copyright IRASS Publisher. All Rights Reserved

identify, evaluate, and compare the key concepts from various previous studies with the views presented by Otero (2018). As such, this paper not only explains the theory and practice of IT auditing, but also provides a critical evaluation of the risks, controls, and auditing techniques such as CAATs in the modern context. The authors also highlight the importance of compliance with regulations and information security standards that are increasingly tightened as concerns about data privacy and security increase. In this writing process, the presentation of a well-structured narrative supported by references from various academic sources ensures that the paper provides a comprehensive view of the challenges facing IT auditors as well as solutions that can be implemented to improve the effectiveness of controls in a dynamic technology environment. The process of revision and editing is also an integral part of this method, with the aim of improving and clarifying the presentation of arguments so that each point raised can be understood clearly and in accordance with high academic standards.

4. Result

4.1 IT Audit and Control Effectiveness in Information Systems Amid Technological Developments

Although information technology offers the potential to improve audit quality, its use also presents new challenges (Nasir, 2023). Auditors must be able to understand the technology used by the companies they audit, as well as ensure that the data used in the audit is reliable and secure (Judijanto, 2024). Additionally, with the ever-evolving complexity of data, auditors need to use appropriate analysis tools and techniques to generate relevant and useful audit findings for their clients. It plays a crucial role in ensuring that an organization's information systems operate safely, reliably, and effectively amid rapid technological developments. In the modern digital era, technologies such as cloud computing, MDM, and IoT have become an integral part of daily business operations. These technologies present a variety of significant benefits, including increased efficiency, flexibility in data storage and processing, and ease of access to information from various devices. However, behind these advantages, there are risks that cannot be ignored. The role of IT auditing is crucial in ensuring that the controls in place are able to identify, manage, and mitigate risks arising from the adoption of this new technology. Otero (2018) emphasizes the importance of audits that focus on evaluating thesecurity, reliability, and integrity of the data processed through these new systems (Tasya Kamila, 2018).

In the context of cloud computing, although these technologies offer great advantages such as reduced infrastructure costs and increased productivity, threats to data security have also increased significantly. Data stored in the cloud resides outside the organization's internal infrastructure, which means unauthorized access or data leakage can occur if security controls are not strictly enforced. Additionally, MDM technology allows employees to use personal devices to access organizational data, which also adds to the risk associated with data loss or misuse if the device is not properly protected. Meanwhile, IoT, with its increasingly widespread connectivity, increases network complexity and creates larger security gaps. Therefore, IT audits must not only evaluate existing controls, but also need to ensure that those controls are able to adapt to the changes brought about by new technologies.

4.2 Risks of Applying Modern Technology and the Role of IT Auditors in Risk Identification and Mitigation

With new risks that can arise anytime and anywhere, new methods of auditing or inspection and control must be introduced. The control here is used to know what method is suitable to use and not to change tools and others. In the application of modern technologies such as ERP and cloud computing, IT auditors have identified several key risks that threaten the security, data integrity, and stability of business operations. ERP, which is designed to integrate various business functions such as finance, human resource management, and supply chain, does provide great benefits in the form of data efficiency and consistency. However, ERP systems can also open up significant risks if not managed properly. Errors in implementation, inadequate configuration, or weak security controls can lead to data leaks, operational disruptions, and inaccurate decision-making based on incorrect data. In addition, cloud computing, with its advantages in terms of flexibility and scalability of data storage, also presents serious challenges related to the security management of data stored on external servers. Cyber threats and the risk of unauthorized access are the main concerns when data is no longer under the physical control of the organization (Febryana Dewi, 2022).

IT audits found that many organizations have difficulty adapting their traditional controls to more advanced technology environments such as ERP and cloud computing. Controls previously designed for internal systems may not be adequate enough in the face of the more complex dynamics of modern technology. For example, in the context of ERP, a lack of strict access controls or monitoring of data modification can result in potential data misuse or manipulation. On the other hand, in cloud computing, the risk increases when organizations fail to verify the security measures implemented by cloud service providers. This can lead to vulnerability to cyberattacks or loss of critical data in the event of a service disruption. Therefore, the role of IT audits is crucial in helping organizations reevaluate and update their controls to match the ever-evolving demands of technology.

4.3 Compliance with Data Privacy Regulations and Their Impact on IT Audits

Based on the analysis conducted, compliance with data privacy regulations, such as the General Data Protection Regulation (GDPR), has a significant impact on IT audits. The GDPR, enforced in the European Union, sets high standards for the management of personal data, requiring organizations to implement strict measures in data protection. For organizations operating within jurisdictions where the GDPR applies, it is important to ensure that they comply with all requirements set forth by these regulations. This includes aspects such as the collection, storage, and use of personal data, as well as the rights of individuals to access, change, or delete their data. In this context, IT audits serve as a tool to assess the extent to which organizations have met these legal requirements, as well as identify gaps or weaknesses in existing policies (Agustinus Wempi, 2024).

The findings from the IT audit show that many organizations face serious challenges in implementing effective policies to ensure that the data they manage is properly protected and complies with applicable laws. One of the main challenges is the lack of a deep understanding of GDPR requirements across all layers of the

© Copyright IRASS Publisher. All Rights Reserved

organization. Often, staff do not have adequate training on data protection and the importance of regulatory compliance. This can result in unintentional privacy breaches, which in turn can result in severe legal sanctions as well as damage to the organization's reputation. Additionally, organizations often lack the resources to implement the controls necessary to meet GDPR standards, such as data encryption, strict access management, and effective oversight.

IT audits not only focus on evaluating regulatory compliance, but also play a role in building awareness across the organization regarding the importance of protecting personal data. By conducting a thorough risk assessment, IT auditors can help organizations identify high-risk areas and recommend necessary corrective measures. In addition, IT audits also serve to ensure that organizations have effective monitoring and oversight processes in place to detect and respond quickly to potential data breaches. With a proactive approach, organizations can reduce the risk of data privacy breaches and ensure that they not only meet regulatory compliance but also build trust among customers and business partners. The active involvement of IT auditors in this process is essential for creating a strong data protection culture within the organization.

5. Discussion

IT auditing has an increasingly crucial role in the midst of rapid technological developments that are changing the way organizations operate. In this context, technologies such as cloud computing, Mobile Device Management (MDM), and IoT have become an integral part of modern business strategies. While these technologies offer many benefits, such as efficiency and flexibility, they also carry significant risks. Therefore, it is important for IT audits to focus on evaluating existing controls, ensuring that they are able to identify, manage, and mitigate risks associated with the adoption of new technologies. Otero (2018) highlights that audits that focus on security, reliability, and data integrity are indispensable to keeping organizational information systems from potential threats (Carlina Sherly, 2024).

In the implementation of ERP systems and cloud computing, IT auditors face challenges in adapting existing controls to an increasingly complex technology environment. ERP systems designed to improve data integration and consistency can present serious risks if not managed properly. For example, a lack of strict access controls can lead to data manipulation that can potentially harm business decisions. Likewise, in the context of cloud computing, the risks associated with data stored on external servers can increase if security measures are not properly implemented. IT audits should serve as proactive watchdogs, helping organizations evaluate and update their controls to align with evolving technology dynamics.

In addition to the challenges faced in managing risks, compliance with data privacy regulations such as the General Data Protection Regulation (GDPR) is also an important focus in IT audits. The GDPR itself was passed and replaced the previous regulation the Directive 95/46/EC. The previous rules were considered less able to provide protection, especially when violations were committed by organizations or companies outside the European Union. In addition, Laura Vegh (2017) responded that the new GDPR is better because it is a regulation rather than a directive, which means that it applies to all EU member states without exception. The GDPR sets high standards for the protection of personal data and requires organizations to implement strict policies. However, findings from IT audits show that many organizations have difficulty implementing such policies. A lack of understanding across layers of the organization

about the requirements of the GDPR, as well as limited resources to implement the necessary controls, can lead to unintentional privacy violations and severe legal sanctions. In this case, IT auditors have a responsibility to not only assess compliance, but also to raise awareness regarding the importance of data protection throughout the organization.

The involvement of IT auditors in audit processes that focus on compliance and risk management is essential for creating a strong data protection culture within the organization. By conducting a thorough risk assessment, auditors can identify high-risk areas and recommend necessary corrective measures. This proactive approach allows organizations not only to meet regulatory compliance, but also to build trust among customers and business partners. Thus, IT audits serve as the vanguard in protecting sensitive data and ensuring that an organization's information systems can operate safely and efficiently in an ever-changing technological era.

Overall, this discussion emphasized the importance of the role of IT audits in managing risk and ensuring regulatory compliance in the context of modern technology. In the midst of rapid development, organizations must be adaptive and responsive to emerging challenges, and IT audits can be a key option in this effort. The active involvement of IT auditors in every step of risk management and compliance will greatly contribute to the sustainability and future operational success of the organization.

6. Conclusion

Thus, it can be concluded that Information Technology (IT) audits play a crucial role in maintaining the reliability, security, and efficiency of information systems in modern organizations. With the rapid development of technologies such as cloud computing, MDM, and IoT, risks to information systems are increasing. Therefore, proper risk control and management is essential to protect sensitive data and ensure compliance with applicable regulations, such as privacy and information security policies. Computer-aided auditing technologies (CAATs) are also increasingly relevant in helping auditors to effectively analyze data and detect potential issues that may have been missed in manual audits. Deep literacy of technology and regulations is a must for IT auditors to perform their duties effectively in an ever-changing environment.

As a suggestion, organizations should continue to develop and update IT control policies and controls along with the adoption of new technologies to minimize risks. IT auditors need to be provided with ongoing training to understand the latest technologies and regulatory changes, as well as utilize computer-aided audit techniques to improve the accuracy and efficiency of the audit process. In addition, risk management and regulatory compliance should be top priorities in any IT management strategy so that organizations can operate safely, efficiently, and in accordance with applicable regulations.

© Copyright IRASS Publisher. All Rights Reserved

References

1. Agustin, Ida. (2024). Teknologi Digital Dan Transformasi Internal Audit Terhadap Perlakuan Laporan Keuangan : Studi Literatur.” Jurnal Mutiara Ilmu. 2(2). 1-15.
2. Dewi, Febryana. 92024). Manajemen Risiko Teknologi Informasi Terhadap Audit Internal dan Dampak yang Ditimbulkan.” Jurnal Sistem Informasi. 4(2).12-24.
3. Farah, Ashma. (2024). Pengaruh Audit Teknologi Informasi Terhadap Kualitas Audit.” Jurnal Fakultas Teknik Informasi. 1(3). 1-18.
4. Kamila, Tasya. (2024). Audit Sistem Informasi terhadap Kemajuan Teknologi.” Diakses pada https://student-activity.binus.ac.id/isgbinus /2018/10/audit-sistem-informasi- terhadap-kemajuan-teknologi/. Pada tanggal 17 Oktober 2024.
5. Karlina, Sherly. (2024). Dampak Teknologi Informasi Mengenai Proses Audit: Teknologi Informasi.” Jurnal Teknik Mesin, Industri, Elektro, dan Informatika. 3(1). 25-38.
6. 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
7. Muhammad, Son. (2024). Analisis Deskriptif: Pengertian, Tujuan, Metode, dan Cara Membuatnya. Diakses pada https://educativa.id/2023/05/31/analisis-deskriptif- pengertian-tujuan-metode-dan-cara-membuatnya/. Pada tanggal 17 Oktober 2024.
8. Nasution, A.A., Erlina, & Atmanegara., A.W (2022). Learning Validation Control and Input Error Correction on Implementation of Computer Assisted Audit Techniques (CAATS) (Review New Trends in Sustainable Development of Learning Education Management Models for the Accounting Student). Webology. 19(1). 1850-1861. DOI: 10.14704/WEB/V19I1/WEB19124. https://www.webology.org/abstract.php?id=887
9. Otero, A. R. (2018). Information technology control and audit (5th ed.). Auerbach Publishers, Incorporated. ProQuest Ebook Central.
10. Pu, G., Wong, W. K., Du, Q., Al Shraah, A., Alromaihi, A., (2024). Asymmetric impact of natural resources, fintech, and digital banking on climate change and environmental sustainability in BRICS countries. Resources Policy, 91, 104872. https://doi.org/10.1016/j.resourpol.2024.104872
11. 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.
12. Wempi, Agustinus. (2024), Regulasi Teknologi Keamanan Siber Sebagai Upaya Mengatasi Ancaman Keamanan Bagi Privasi Di Era Digita.” Jurnal Hukum Sehasem. 10(2). 509-516.
13. Wijoyo, Agung. (2023). Pengaruh Sistem Informatika terhadap Efisiensi Operasional Perusahaan.” Jurnal Teknologi, Bisnis, dan Pendidikan. 1(2).s 1-8.
14. Yohanes, Hermanto. (2019). General Data Protection Regulation dan Kedaulatan Negara Uni- Eropa.” Jurnal Law Review. 2(2). 60-71.

© Copyright IRASS Publisher. All Rights Reserved