Bima Journal – Bussiness Management and Accounting
Available online at : http://journal.pdmbengkulu.org/index.php/bima
DOI: https://doi.org/10.37638/bima.7.1.547-556

Digital Audit as a Solution to Data Security Challenges in the Era of Digital Transformation

Mitrah Andira[1*]; Andika Rusli[2]; Andi Dahri[3]

[1,2,3]***Faculty of Economics and Business, Muhammadiyah University of Palopo***

*Correspondent Author:mitraandiraa@gmail.com**

How to Cite :
Andira, M., Rusli, A., Dahri, A. (2026). Digital Audit as a Solution to Data Security Challenges in the Era of Digital Transformation. *Bima Journal : Business, Management and Accounting Journal, 7* (1) 547-556. DOI: https://doi.org/10.37638/bima.7.1.547-556

ARTICLE HISTORY
Received [15 January 2026]
Revised [20 January 2026]
Accepted [11 June2026]

KEYWORDS
Digital audit; data security; digital transformation;

ABSTRACT

Purpose: *This study aims to examine the role of digital audits as a solution to data security challenges in the era of digital transformation, with a case study of the Palopo City Communication and Informatics Agency (Kominfo) in 2025. In the context of implementing an Electronic-Based Government System (SPBE), data security is a crucial aspect that demands systematic oversight through digital audits.* ***Methodology:*** *This study uses a qualitative method with a case study approach, involving two key informants from the IT field to gain an in-depth understanding of digital audit implementation, security strategies, and regulatory compliance.* ***Results:*** *The results show that digital audits play a crucial role in ensuring data confidentiality, integrity, and availability through the implementation of firewalls, VPNs, layered authentication systems, structured backups, and the use of technology-based audit tools. In addition to technical aspects, digital audits also strengthen compliance with regulations such as the Personal Data Protection Law (UU PDP) and the National Cyber and Crypto Agency (BSSN) guidelines.* ***Findings:*** *The findings confirm that digital audits serve as a strategic instrument for maintaining data security and enhancing institutional accountability.* ***Novelty & Originality:*** *This study offers novelty by examining digital audit implementation in a local government context in Palopo City, an area rarely explored in prior research.* ***Conclusions:*** *In conclusion, digital audits have proven to be a strategic instrument for maintaining data security and increasing public trust in government digital services, while also serving as an implementation model that can be replicated by other agencies in the era of digital transformation.* ***Type of Paper:*** *This paper is an empirical research paper.*

INTRODUCTION

In the era of growing digital transformation, organizations worldwide face significant challenges in managing and protecting their data. Digitalization has brought benefits such as increased operational efficiency, easier access to information, and the ability to analyze data at scale. However, with this convenience comes serious risks such as cyberattacks, data breaches, and

privacy breaches.(Agustin, 2024)This situation requires special attention to ensure data security and integrity are maintained.

One solution that is starting to gain attention is the digital audit, a systematic process aimed at assessing data security and compliance with applicable regulations. A digital audit assesses not only technical aspects but also the organization's policies, procedures, and culture regarding information security.(Okinaldi & Aziza, 2024). With digital audits, organizations identify security gaps and strengthen data protection across the board.

According to a recent report, numerous organizations have suffered financial and reputational losses due to data security incidents. This phenomenon also includes government agencies such as the Ministry of Communication and Informatics (Kominfo), demonstrating that cybersecurity is a critical priority for Kominfo in protecting its data and information systems, especially following a data breach involving the personal data of millions of Indonesians.(Agustin, 2024).

The Ministry of Communication and Informatics (Kominfo), which has now changed its name to the Ministry of Communication and Digital (Komdigi) at the central level, is a government agency with strategic responsibility for managing the communications and informatics sector in Indonesia. This institution plays a crucial role in establishing policies and overseeing broadcasting, telecommunications, and multimedia services, with the primary goal of ensuring information can be disseminated quickly, securely, and equitably throughout the country. Komdigi also focuses on developing digital infrastructure, public digital literacy, and cybersecurity, which are crucial pillars in supporting digital transformation and technology-based economic progress in Indonesia.

In an effort to improve digital governance, the Indonesian government has developed an Electronic-Based Government System (ESBS) policy. ESBS encompasses the integrity of government information systems and business processes that utilize information technology comprehensively to improve the efficiency, effectiveness, transparency, and accountability of public services. A key component of ESBS implementation is information security, which aims to protect data and electronic systems from various threats, both internal and external. To this end, the government has established a national ESBS architecture, including information security standards that adhere to risk management principles and rigorous data protection practices.

In the increasingly digital era, personal data breaches remain a serious challenge for the government and organizations in Indonesia. Several high-profile cases, such as the leak of prepaid SIM card registration data and Indihome customer data, have highlighted the weaknesses of existing security systems and raised public concerns about the protection of personal information.(Parsaorantua et al., 2017)The risk of data misuse by irresponsible parties is increasing and eroding public trust in the government's ability to secure personal data.(Khotimah & Ula, 2023).

Therefore, it is important to understand how digital audits can be integrated into organizational risk management practices. This research aims to explore the experiences and perspectives of professionals involved in the digital audit process to provide practical recommendations for organizations adopting digital audits as part of their data security strategy.

In addition, this study also highlights various challenges in implementing digital audits, such as limited resources, lack of technical knowledge, and resistance to change.(Digital: et al., 2023)By understanding these challenges, this research is expected to provide solutions that can help organizations optimize the implementation of digital audits as part of their data security strategy.

The novelty of this research lies in the qualitative approach which emphasizes practical experience and human perspective, in contrast to previous research which focused on technical and regulatory aspects.(Rahmasari, 2023)By involving various stakeholders, this research is expected to provide a comprehensive overview of the application of digital audits to strengthen data security.

This research is also relevant to the increasing prevalence of data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe and the Personal Data Protection Act in Indonesia. Digital audits play a critical role in ensuring organizational compliance with these regulations and helping assess the effectiveness of personal data management.(Kautsar, 2022).

Furthermore, this study examines the role of technologies such as artificial intelligence and data analytics, in supporting digital audit processes to be more efficient and effective.(Nsafe et al., 2021)Thus, this research is expected to provide theoretical and practical contributions in efforts to strengthen data security in the era of digital transformation.

This research focuses on how the implementation of SPBE in the Palopo City Communication and Information Technology Agency (Kominfo) maintains data security and reduces cyber threats, with digital audits as an approach to assess the effectiveness of the system.

A digital audit is an evaluation process that uses technology to verify the reliability, security, and compliance of digital data. Unlike traditional audits, which tend to rely on manual methods, digital audits can process large amounts of data (big data) quickly and efficiently. In the digital era, digital audits have become a crucial component in ensuring that an organization's information technology systems are functioning properly and securely.

Implementing digital audits requires investment in software, auditor training(Okinaldi & Aziza, 2024)The main factors influencing successful implementation include cost, the company's technological readiness, and the auditor's competence in using new technology. Selecting the right technology for a digital audit depends on the type of data being audited, regulatory requirements, and compatibility with existing systems.(Fajrillah et al., 2024).

For example, blockchain is being used to increase transparency in financial transaction audits, while AI (Artificial Intelligence) and Machine Learning help detect anomalies in financial reports. Furthermore, digital audits also enable proactive risk management by leveraging predictive analytics. Through Machine Learning algorithms, auditors can identify potential threats based on historical data patterns.(Digital: et al., 2023)This approach provides added value because organizations can identify risks before they develop into real threats.

Key Characteristics of Digital Audit:

a. Real-Time Monitoring: Allows for real-time identification of suspicious activity.
b. Use of Big Data Analytics: Able to analyze large amounts of data to detect anomalous patterns.
c. Transparency through Blockchain: Provides an immutable audit trail, increasing accuracy and trust.
d. Predictive Analytics: Using Machine Learning to predict risks based on historical data.
e. Digital Audit Implementation: Factors that influence the success of digital audit implementation include costs, technology readiness, and auditor competence.(Fajrillah et al., 2024). Selecting the right technology is crucial to achieving the desired results.

Based on the discussion of the key characteristics of digital audits, including real-time monitoring, big data analytics, transparency through blockchain, and predictive analytics, the question arises as to whether the implementation of these technologies has been effective in the institutions studied. To what extent are these characteristics able to help organizations anticipate risks and accurately detect anomalies?

Data Security Challenges

In the era of digital transformation, data security challenges are increasingly complex and diverse. Threats such as malware and ransomware continue to increase, threatening the integrity and confidentiality of organizational data. Data breaches, whether due to cyberattacks or human error, can damage reputations and customer trust.

In addition, non-compliance with data protection regulations such asGDPRand the California Consumer Privacy Act (CCPA) Security is a critical issue for organizations to address, as violations can result in severe legal penalties. Lack of security awareness among employees is also a challenge, and training and education on good security practices are essential to mitigate the risks posed by human error.(Mirwali Azizi et al., 2024).

Meanwhile, digital audits face unique challenges amidst increasing system complexity. Auditors need to possess adequate skills and knowledge to handle new technologies and integrate

data from multiple sources. Data security during the audit process is also a key concern, with the use of encryption technology and strict access controls crucial to protect sensitive information.(Saeed, SaqibSaeed, S., Altamimi, A., & Alqahtani et al., 2023). Furthermore, ensuring that digital audits comply with applicable standards and best practices is a challenge that must be addressed, so certification and independent audits can help maintain compliance and improve the effectiveness of the audit process.

After understanding the complexity of data security challenges such as malware attacks, information leaks, and regulatory non-compliance, it's interesting to examine how digital audits can help address these issues. Can digital audits be an effective solution for maintaining data confidentiality, integrity, and availability amidst the rise of cyberthreats?

The Relationship between Digital Audit and Data Security Challenges

Digital audits play a critical role in helping organizations address data security challenges. By leveraging advanced technology, digital audits can provide a more systematic, data-driven approach to protecting an organization's sensitive information.(Digital: et al., 2023)Through the use of real-time monitoring and analytics tools, digital audits can identify suspicious behavior patterns and potential threats before they escalate into larger problems.

Additionally, digital audits enable organizations to conduct comprehensive risk assessments, allowing them to allocate resources more efficiently to address the most vulnerable areas. Thus, digital audits serve not only as an evaluation tool but also as a proactive mechanism that helps organizations build resilience against evolving data security threats.(Digital: et al., 2023).

This is also reinforced by research(B & Rusli, nd). which shows that strengthening internal controls and implementing probity audits simultaneously play a significant role in preventing fraud, particularly in the procurement of goods and services in the public sector. Audit mechanisms that emphasize transparency, integrity, and accountability have been shown to detect potential irregularities early and strengthen an organization's internal oversight system. This finding aligns with the concept of digital auditing discussed in this study, where the use of audit technology can strengthen oversight effectiveness and safeguard data security from the risk of misuse or information leakage.

The relationship between digital auditing and data security challenges has been conceptually outlined. However, to what extent is this relationship realized in practice? Do digital audits actually have a tangible impact on supporting data protection and improving compliance with applicable security regulations?

The Contribution of Digital Audits to Addressing Data Security Challenges

Digital audits make a significant contribution to addressing data security challenges in several ways. First, they enable early threat detection by monitoring activity in real time, allowing potential threats to be identified before they become major problems.

The use of Intrusion Detection Systems (IDS) is a concrete example of how suspicious activity can be automatically detected and reported. Furthermore, digital audits also help organizations ensure compliance with applicable regulations. By automating the verification and reporting processes, organizations can more easily monitor compliance with established data security standards.

Furthermore, digital auditing supports proactive risk management through data-based predictive analytics.*machine learning*, which allows identification of potential risks based on historical data patterns.(Rahmasari, 2023)This provides an opportunity for organizations to take preventive action to reduce potential risks.

Furthermore, digital audits improve the efficiency of the audit process by enabling faster and more efficient audit completion, particularly in big data processing, thereby reducing costs and time. Finally, by providing a transparent audit trail and proof that data security systems have been

thoroughly tested, digital audits help organizations build trust with customers, business partners, and regulators.

Several previous studies have explored the relationship between digital auditing and data security challenges. One such study is by(Alzahrani & Alshahrani, 2020) discusses the role of digital audits in improving data security by identifying vulnerabilities and providing recommendations for improvement. This study also highlights the challenges organizations face in implementing digital audits.

Besides that,Manita, R., Elommal, N., Baudier, P., & Hikkerová, (2020)In their article they analyze the impact of digital transformation on audit practices, showing how digital auditing can help organizations address the data security challenges that arise from digitalization.Saeed, SaqibSaeed, S., Altamimi, A., & Alqahtani et al., (2023)presents a case study of the cybersecurity challenges faced by organizations when implementing digital audits, and provides recommendations for improving data security in the audit context. Research bySlapničar, S., Vuko, T., Čular, M., & Drašček, (2022)evaluate the effectiveness of digital audits in reducing the risk of data breaches and improving compliance with data security regulations. Finally,Krieger, F., Drews, P., & Velte, (2021)demonstrates how the implementation of digital audit tools can improve data security and audit efficiency in organizations, while identifying the challenges faced in their implementation.

The contributions of digital auditing have been theoretically explained, both in terms of early threat detection, regulatory compliance, and audit process efficiency. The question is, to what extent are these contributions implemented in the institutions studied? Is digital auditing truly capable of providing effective and sustainable solutions to data security challenges? These studies provide a strong foundation for understanding the context and challenges faced in implementing digital audits as a solution to data security issues.

METHOD

Analysis Method

The research method used by the researcher is a qualitative study centered on case studies to in-depth investigate how digital audits are implemented as a solution to data security challenges in government agencies undergoing digital transformation. This approach was chosen to enable the researcher to understand the processes, techniques, experiences, and perceptions of the parties involved in implementing digital audits. This method selection is also relevant to questions raised in the literature review, such as the extent to which digital audit characteristics are implemented, how digital audits address data security challenges, and their contribution to supporting regulatory compliance.

This research will be conducted at a government agency that has implemented digital audits or is currently undergoing a digital transformation. The location and timing of the research will be determined based on the access and willingness of participants to participate.

The subjects in this study consisted of several relevant parties, namely the IT or cybersecurity team, managers or heads of related units, as well as audit documents and the organization's data security policies. Subject selection was conducted using purposive sampling, selecting participants with direct experience in digital audits and data security management, thus providing in-depth and relevant information to the research focus. This aligns with the research objective of answering conceptual questions from the literature review, for example, regarding the effectiveness of digital audit implementation, strategies for addressing cyber threats, and the impact of digital audits on regulatory compliance.

The data in this study were collected through observation and in-depth interviews. Researchers conducted direct observations to determine how companies or agencies implement digital audits or are currently undergoing digital transformation in their data security systems, as

well as the extent to which digital audit technology has been integrated to address information security challenges. The second technique involved interviews with informants directly involved in the digital audit process or currently undergoing digital transformation to explore their understanding of the issues formulated in the literature review, such as the use of big data analytics, the implementation of real-time monitoring, and the contribution of digital audits to risk mitigation.

Operational definitions of variables are used to explain the boundaries and indicators of the variables being studied. The operational definitions of the variables in this study are presented in Table 1.

Table 1. Operationalization of Variables

Variables	Variable Definition	Indicator
Digital Audit (X)	A digital audit is an information technology-based evaluation process that aims to assess the effectiveness of internal controls, policy compliance, and data management in SPBE.	1. SPBE data confidentiality protection policy. 2. Data integrity control from unauthorized changes. 3. System readiness ensures the availability of SPBE services. 4. Effectiveness of SPBE service authentication system.
Data Security (Y)	Efforts to protect SPBE data to keep it safe and accountable	1. Technical procedures to maintain data confidentiality. 2. Mechanism to maintain data integrity. 3. Service backup and recovery system. 4. Implementation of operational authentication. 5. Non-repudiation guarantee through activity logging.

Source : Data processed, 2025

Based on Table 3.1, the Digital Audit and Data Security variables are described through several indicators which form the basis for compiling interview guidelines in this study. To ensure data validity, this study employed triangulation techniques. Triangulation was conducted from three perspectives: source triangulation, which compared data from various sources; technical triangulation, which compared interview and observation results obtained from different sources; and temporal triangulation, which collected data over different time periods to ensure consistency of the information obtained.

The data analysis technique was conducted thematically in three stages: data reduction to sort out important information related to the research focus of digital audit and data security, data presentation in narrative form or a thematic matrix, and drawing conclusions. The analysis process was directed at answering the issues formulated in the literature review, including questions that connect between sub-chapters, so that the research results can provide concrete answers regarding the effectiveness of digital audits, their relationship to data security challenges, and their contribution to regulatory compliance and risk mitigation.

RESULTS AND DISCUSSION

This study aims to understand how digital auditing plays a role in maintaining data security in the era of digital transformation, using a case study of the Palopo City Communication and Informatics Agency (Kominfo). Through in-depth interviews with two key informants from the IT sector, the study found that digital auditing plays a crucial role in maintaining data confidentiality, integrity, and availability, while ensuring compliance with applicable regulations in the implementation of the Electronic-Based Government System (SPBE).

Based on interviews, it was discovered that the implementation of digital audits at the Palopo Ministry of Communication and Information Technology (Kominfo) focuses on the SPBE system, which integrates various public services such as population data, medical records, and government administration. Because this system handles sensitive data, security is implemented in layers, including firewalls, a Virtual Private Network (VPN), and a two-factor authentication system. These results indicate that digital audits are used not only as a technical audit tool but also as a crucial part of a data protection strategy.

The IT Manager of the Ministry of Communication and Information Technology, Mr. Ramlan, stated that all digital security and audit policies are always guided by the Personal Data Protection Law (PDP Law) and guidelines from the National Cyber and Crypto Agency (BSSN). He explained:

"Regarding data confidentiality, we continue to adhere to the Personal Data Protection Act. That serves as our guidance and reference. We also have SOPs and a personal data security system specifically regulated for population data and medical records."

Based on this statement, it can be interpreted that the implementation of digital audits within the Palopo Ministry of Communication and Information Technology (Kominfo) environment emphasizes not only technical aspects but also regulatory aspects, which are the primary basis for data protection. This demonstrates a synergy between technological approaches and legal compliance. This finding aligns with the perspective of(Agustin, 2024)which emphasizes that digitalization is not enough just by modernizing the system, but must also be supported by a strong data protection policy to ensure the security of public information is maintained.

Furthermore, the informant added that in the SPBE digital audit, security is implemented not only at the application level but also encompasses the infrastructure or backend of the system. He explained,

"There are several procedures within the system that we must understand. The first relates to who is allowed access, followed by firewall and VPN protection. Two-factor identification is available upon login, for example, through a notification to verify the credibility of the user accessing the service."

Based on these results, it can be understood that digital audits serve as a comprehensive control mechanism, not only evaluating system performance but also ensuring that each user follows standard security procedures. This principle aligns with the CIA Triad (Confidentiality, Integrity, and Availability), which emphasizes data protection in terms of confidentiality, accuracy, and availability.

Furthermore, interviews also revealed that infrastructure readiness and role allocation within the IT team influence the success of digital audit implementation. The informant explained,

"We ensure our data center infrastructure is in good condition. At Kominfo, we have an IT team that provides backup, divided into divisions: programming, network, and security."

From this statement, it can be seen that Kominfo has implemented a structured work system with a clear division of responsibilities, so that each section can focus on maintaining and securing the system.

From a regulatory perspective, all audit activities also adhere to the SPBE indicators and guidelines established by the central government. The informant emphasized,

"SPBE has a set of standards. Of the 47 existing indicators, all have standards, including how we implement this audit system to ensure all stages and procedures comply with regulations."

These findings show that digital audits at the Palopo Ministry of Communication and Information Technology not only assess technical effectiveness but also ensure that the system operates in accordance with applicable SPBE regulations.

Furthermore, research results show that the use of audit tools is a factor that increases the efficiency of the audit process. The informant explained,

"When conducting an audit, we use audit tools. This is important because it can speed up the audit process and increase the accuracy and transparency of audit results."

Based on this interpretation, it can be concluded that the use of audit tools helps auditors in collecting, analyzing, and reporting data more systematically. This is in line with the findings.(Rahmasari, 2023)which states that the use of technology in digital audits can increase the speed and accuracy of audit results.

Interviews also revealed that digital audits at the Ministry of Communication and Information Technology (Kominfo) have comprehensively implemented the principles of Confidentiality, Integrity, and Availability. To maintain data confidentiality, Kominfo utilizes the HTTPS protocol and a Role-Based Access Control (RBAC) system that limits user access rights according to their responsibilities. To maintain data integrity, information is classified based on sensitivity levels, such as public, restricted, confidential, and strategic data. The informant explained,

"In each category, for example, there's public data, restricted data, confidential data, and then there's strategic national data. All of this is implemented in the application system."

This classification demonstrates that the security system at Kominfo operates according to the principle of integrity, where each piece of data is treated differently based on its importance. Furthermore, to ensure data availability, a multi-layered backup system is implemented at both the National Data Center (PDN) and the Palopo Kominfo DNS. The informant stated,

"There cannot be just one backup system. There must be more so that there is no data loss. AI performs backups every week and also reports the results."

Based on the interpretation of these results, it can be concluded that the Ministry of Communication and Information Technology has developed a robust security system through a layered approach, encompassing infrastructure, backup systems, and the division of roles between teams. This strategy reflects the concrete application of the CIA Triad principle in maintaining the sustainability of digital services.

However, this study also found that there are still challenges in implementing digital audits, particularly in the human resources aspect. Informants mentioned that there are still obstacles in implementing user authentication, with many users having difficulty creating complex passwords or frequently forgetting them. They said,

"I still often forget my password and have difficulty with the level of difficulty of the password which must be a combination of numbers, letters, and symbols."

This shows that the human factor is still a weak point in data security, so there is a need for ongoing education and assistance.

To support system accountability and transparency, the Kominfo SPBE is also equipped with an activity log mechanism that records all user activity. The informant explained,

"On the server side, there's an activity log that records all user activity for each access role. Each application also has additional tools that can track user activity while using the application."

Based on these results, the implementation of activity logs can be understood as a form of oversight and proof of user accountability for their actions. In theory, this supports the principle of non-repudiation and strengthens digital auditing as an information system control instrument.

Overall, the results of this study indicate that digital audits at the Palopo Ministry of Communication and Information Technology have been implemented comprehensively and

effectively. Digital audits serve not only as a technical evaluation tool but also as an oversight mechanism that ensures regulatory compliance and improves work efficiency. The application of the CIA Triad principles has proven effective in maintaining data security, while regulatory support and SPBE policies strengthen the accountability of public agencies. While challenges remain in terms of human resources and security awareness, digital audits have become a strategic instrument in strengthening public trust in government digital services.

This finding supports the view(Agustin, 2024)And(Rahmasari, 2023)that the success of a digital audit is not only determined by the technology used, but also by the integration between policies, regulations, and the readiness of human resources in the era of digital transformation.

REFERENCES

Agustin, S. (2024). The Impact of Advances in Information Technology in the Digital Era on Personal Data Security: Challenges and Countermeasures Against Cybercrime. 1(6), 500–504.

Alzahrani & Alshahrani (2020). Digital Footprint Analysis: Understanding the Role of Audit Evidence in the Big Data Era Ari. Musytari*: Management, Accounting, and Economics Balance Sheet*, 3(2), 1–19.

B, TM, & Rusli, A. (nd). The Influence of Internal Control and Probity Audit on Fraud Prevention in Procurement of Goods and Services (Study at the Palopo City Inspectorate Office). 54, 154–168.

Fajrillah, Baridah, L., Aini, SN, Salsabila, N., & Daulay, MEM (2024). Financial Information System Auditing Process and Opportunities in the Digital Era. INNOVATIVE: Journal of Social Science Research, 4(2), 5544–5554.

Kautsar, TR (2022). A Structured Literature Review of Personal Data Leaks and Personal Data Protection Regulations. 1–101.

Khotimah, K., & Ula, DM (2023). Triwikrama: Journal of Social Sciences. Triwikrama: Journal of Social Sciences, 01(11), 40–50.

Krieger, F., Drews, P., & Velte, P. (2021). Explaining the (non-) adoption of advanced data analytics in auditing: A process theory. International Journal of Accounting Information Systems, 41, 100511.

Manita, R., Elommal, N., Baudier, P., & Hikkerová, L. (2020). The digital transformation of external audit and its impact on corporate governance. Technological Forecasting and Social Change, 150, 119751.

Mirwali Azizi, Hakimi, M., Frishta Amiri, & Amir Kror Shahidzay. (2024). The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges. Open Access Indonesian Journal of Social Sciences, 7(2), 1473–1482. https://doi.org/10.37275/oaijss.v7i2.230

Nsafe, E., No, V., Fitrianingsih, SK, Az, T., & Khadijah, Z. (2021). Proceedings of the National Seminar on Accounting, Finance, Implementation of Computer-Assisted Audit Techniques in the Digital Era. 1(2), 221–227.

Okinaldi, J., & Aziza, N. (2024). Implementation of Audit Technology in the Digital Era. Scientific Journal of Management, Economics, & Accounting (MEA), 8(2), 146–159. https://doi.org/10.31955/mea.v8i2.4016

Parsaorantua, P. humisar, Pasoreh, Y., & Rondonuwu, sintje A. (2017). Implementation of information and communication technology. Acta Diurna, VI(3), 1–14.

Rahmasari, S. (2023). Business Adaptation Strategy in the Digital Era: Navigating Change and Improving Organizational Success. Karimah Tauhid, 2(3), 622–636.

Saeed, SaqibSaeed, S., Altamimi, A., & Alqahtani, M., Altamimi, S.A., Alkayyal, N.A., Alshehri, E., & Alabbad, D.A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15), 1–20. https://doi.org/10.3390/s23156666

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audits. International Journal of Accounting Information Systems, 44, 100548.