JDBIM
(Journal of Digital Business and Innovation Management)

Volume 3, Issue 2, December 2024, 101- 113
ISSN (Online): **2962-3898**
DOI: 10.26740/jdbim.v3i2
https://ejournal.unesa.ac.id/index.php/jdbim

Cyber Security Risk Management Practices: Insights From an ISO 27001 Certified Organization

Shevani Resta Maulana Putri[1]*, Marceli Putri Bernandy [2], Cindy Aulia [3], Muhammad Ghaza Raihan Fikri[4], Javanie Jasmine[5],

[12345]Department of Digital Business, Faculty of Economics, Universitas Negeri Surabaya
Jalan Ketintang, Surabaya 60231, Indonesia
shevaniresta.22020@mhs.unesa.ac.id,

Abstract

In the increasingly complex and dynamic digital era, cybersecurity risk management has become a critical aspect affecting the operations and sustainability of organizations. This study examines the practice of cybersecurity risk management from the perspective of organizations that have obtained ISO 27001 certification, an international standard that sets the criteria for information security management systems (ISMS). The focus of this research is ISO 27001, one of the world's leading information security standards. This study explores the meaning of ISO 27001, risk management, and the process of implementing this certification within organizations through a literature review. Findings indicate that the implementation of ISO 27001 has a significant impact on the organization's awareness of information security management. The implementation process of ISO 27001 includes a series of steps and approaches designed to help organizations effectively manage cybersecurity risks. This study highlights the importance of implementing ISO 27001 into cybersecurity risk management practices to enhance information security and prevent cyber threats. The study also evaluates the level of organizational awareness of the ISO 27001 standard and its impact on the implementation of cybersecurity risk management practices. Our findings show that organizations with ISO 27001 certification have a higher awareness of the importance of cybersecurity risk management, thereby supporting the implementation of more effective risk management practices. This study aims to provide insights and practical guidance for

organizations in applying and utilizing cybersecurity risk management according to the ISO 27001 standard. Therefore, this research contributes to the enhancement of awareness and the implementation of better information security standards in the current digital era.
Keywords: *Cybersecurity Risk Management; ISO 27001; ISO Implementation; Information Security; Organizational Awareness.*

INTRODUCTION

According to Anwar and Gill (2021) risk management in the context of an organization's need to understand the organizational context, stakeholder needs, and expectations is an important approach in ensuring that organizations can identify, assess, and manage risks associated with personal information efficiently and effectively. Risk management aims to optimize results by minimizing negative risks and maximizing positive opportunities. While Information security management is a structured, cost-effective, and systematic approach to establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security through the adoption of an Information Security Management System (ISMS). ISMS helps organizations of any size and industry to protect their information in a planned and affordable way (Junaid, 2023). Risk management and information security management are interrelated because information security risk management involves the process of identifying, evaluating, and managing risks that can affect operational sustainability and corporate reputation related to information security. By implementing information security risk management, organizations can identify potential information security threats, evaluate their impact, and develop strategies to mitigate those risks, thereby helping to protect information from attacks and losses that may occur (Junaid, 2023). Information protection should also be emphasized by implementing administrative, technical, physical, and legal security controls in accordance with privacy principles. Organizations need to define, establish, and implement appropriate security controls across all domains of practice to protect the information being processed (Allendevaux, 2021).

Awareness of the importance of risk management is essential in the protection of personal data and information security, especially in the growing digital era. Organizations need to increase awareness and implementation of risk management at various levels, both state and federal, to protect the security and privacy of citizens. One of the security management systems with international standards is ISO 27001. According to Liao and Chueh (2012) ISO 27001 is an international standard for information security management that specifies the requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS) within an organization. This standard is designed to help organizations protect critical information and effectively manage information security risks. Cyber security risk management and insights from

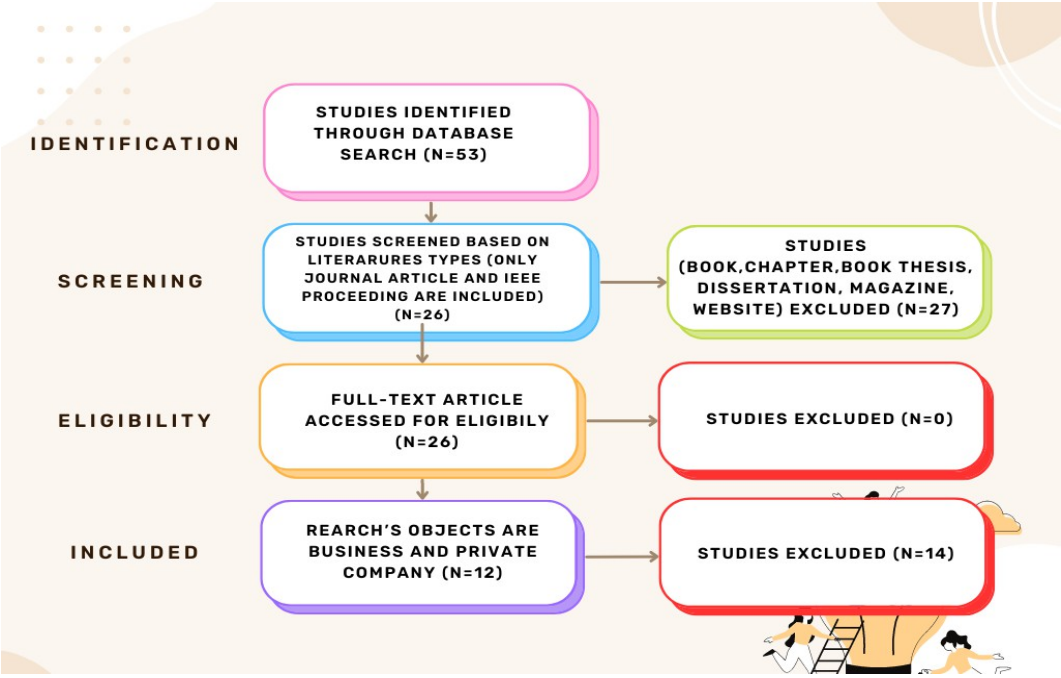
ISO-certified organizations are critical to an organization because they help protect a company's information, assets, and reputation from security attacks that can be economically and reputationally damaging from forms of information security threats including cyberattacks such as malware, phishing, ransomware, DDoS attacks, data theft, and insider threats (Junaid, 2023). These threats can be economically and reputationally costly for an organization if not properly addressed. By implementing cyber security risk management practices and the ISO 27001 standard, organizations can identify, evaluate, and manage information security risks in a systematic and

structured manner, thereby improving overall information security. In addition, ISO 27001 certification also provides confidence to clients, business partners, customers and shareholders that protective measures have been taken to safeguard the organization's assets.

To establish an information security management mechanism based on the ISO27001 standard, some of the efforts and undertaken include drafting and establishing an information security policy that complies with the requirements of the standard, having strict operational procedures to ensure systems that process personal data are subject to security principles, implementing security controls in the system development cycle, ensuring that third-party vendors used by the organization are also subject to sufficiently high security standards, and measuring and evaluating the organization's level of compliance with the requirements of the ISO27001 standard (Allendevaux, 2021).

Thus, cyber security risk management and insights from ISO-certified organizations are critical to maintaining operational continuity and corporate reputation.

METHODS



This research method uses PRISMA, which is a guide used to assess systematic reviews and/or meta analyses. PRISMA assists authors and researchers in preparing a quality systematic review and meta analysis with the steps shown in the following chart:

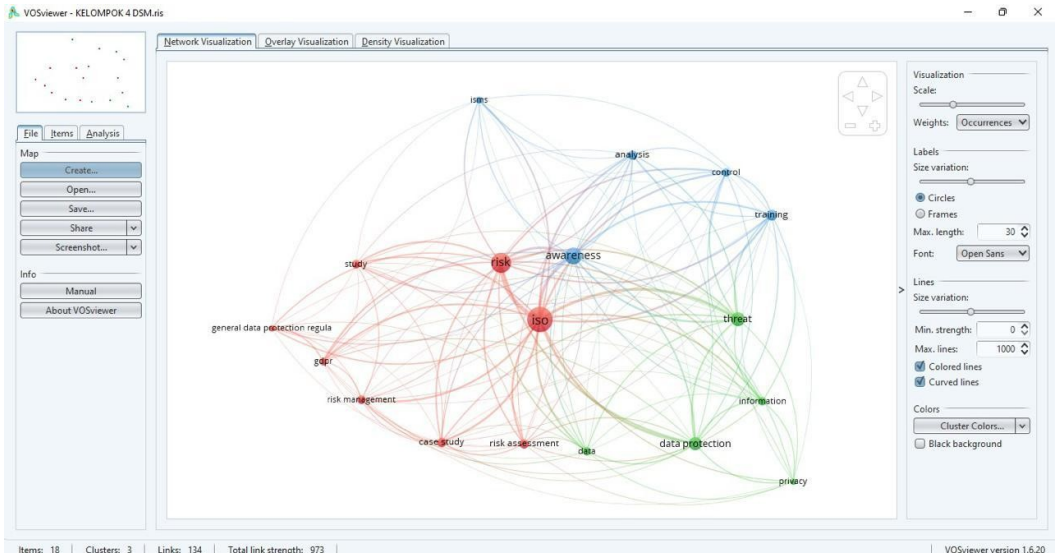


Figure 1. Network Visualization

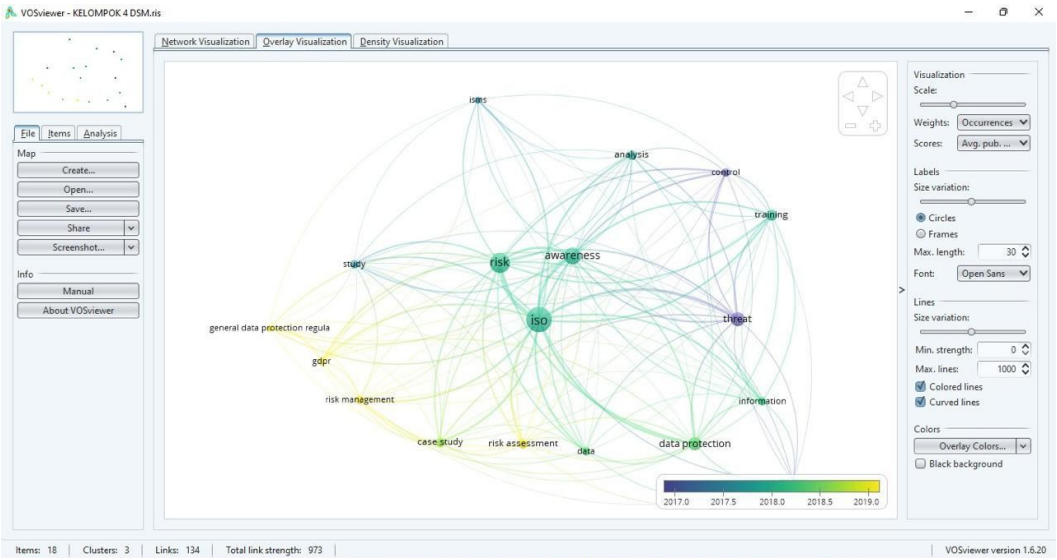


Figure 2. Overlay Visualization

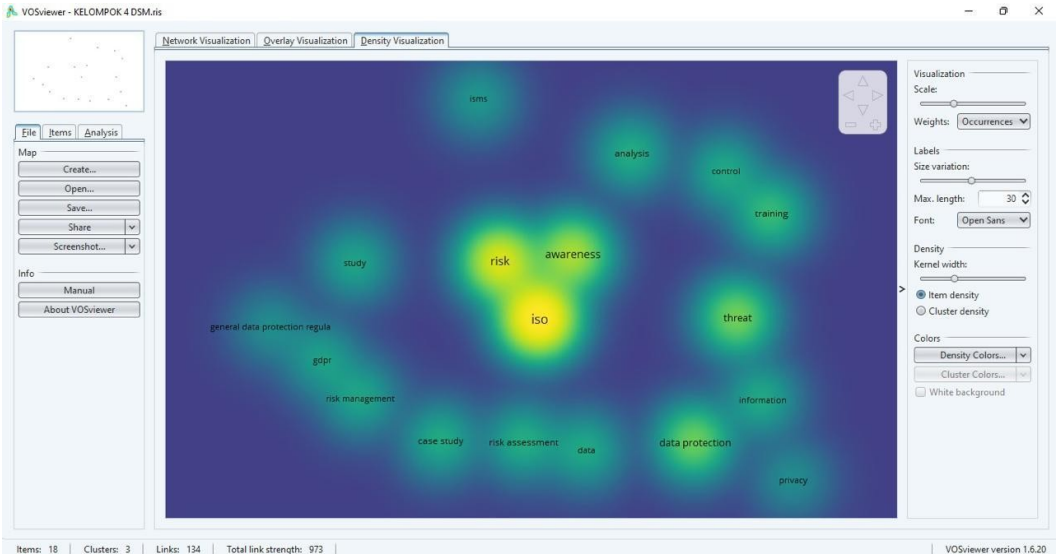


Figure 3. Density Visualization

RESULT AND DISCUSSION

Definition of Data Security Management

In today's business context, data security, better known as data security, should not be ignored. With the increasing complexity of cyber threats, data protection is becoming a top priority for every organization. Various strategies are used, such as encryption, authentication, access control, data backup, and the use of firewalls, all of which are crucial foundations in building defenses against harmful cyberattacks.

Aside from the attack prevention aspect, it is important to note that data security also has a significant impact on maintaining company productivity and strengthening consumer confidence. With a well-integrated security system, organizations can run their operations without the fear of disruption caused by damaging cyberattacks. Furthermore, effective data protection can improve a company's image in the eyes of customers, demonstrating the company's commitment to maintaining the confidentiality and security of the information they manage.

ISO 27001

ISO 27001 is an international standard that specifies the requirements for an Information Security Management System (ISMS) within an organization. This standard provides a comprehensive framework for managing information security and protecting organizational information assets from various cyber security threats and risks (Al-Mayahi, I., & Sa'ad, P. M, 2012). Meanwhile, according to Junaid (2023) ISO 27001 is an international standard for Information Security Management Systems (ISMS) that provides a structured and systematic framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security in an organization. ISO 27001 helps organizations protect their information in a planned and affordable way. So it can be concluded that ISO 27001 is an international standard for Information Security Management Systems (ISMS) that provides a comprehensive framework for managing information security in an organization.

This standard helps organizations identify, evaluate, and manage information security risks that can affect operational sustainability and corporate reputation. By implementing ISO 27001, organizations can ensure that their information systems are

effectively protected from security threats. ISO 27001 certification also provides additional benefits such as improved operational efficiency, reduced costs due to security incidents, and enhanced corporate reputation. Thus, ISO 27001 certification is an important step to help organizations manage information security risks in a more effective and structured. The security objectives of ISO 27001 are to ensure the confidentiality, integrity, and availability of information, while the protection objectives are to prevent unauthorized access, ensure information is not unlawfully altered, and ensure information is available when needed. ISO 27001 also aims to manage information security risks by implementing organizational, human, physical, and technological controls, for which the certification process for ISO 27001 involves several steps. First, the organization needs to define the scope of its Information Security Management System (ISMS) by conducting an initial assessment, requirements analysis, risk management planning, and management evaluation. Next, the organization will undergo a pre-certification audit and assessment to ensure that their processes are compliant with the standard. After that, organizations will receive an official ISO 27001 certificate for their ISMS, which has a validity period of three years. Organizations can also apply for recertification after the certificate expires. The ISO 27001 standard is recommended for implementing an Information Security Management System (ISMS) to address security risks. Integration of safety requirements with security threats is proposed for better management. The references provided provide more information on ISO standards and case studies related to cyber security and safety (Junaid, 2023). The benefits of obtaining ISO 27001 certification include substantial economic and reputational benefits. This certification helps to reduce economic and reputational losses due to security attacks, as well as provide confidence to clients, business partners, customers, and shareholders that protective measures have been taken to safeguard the organization's assets in the case of a security attack.

ISO 27001 certification can also improve an organization's overall structure, help avoid regulatory fines, and reduce the need for frequent audits. Thus, the benefits of obtaining ISO 27001 certification include asset protection, enhanced reputation, and compliance with internationally recognized information security standards.

Definition of Risk Management

Definition of risk management according to experts, understanding Herman Darmawi's definition of risk management is an effort to find out, analyze and control risks in every company activity with the aim of obtaining higher effectiveness and efficiency. Meanwhile, the opinion of economist Joseph Dorfman defines risk management as a logical process to understand exposure to a loss.

Risk is defined as an opportunity for an unwanted, or unexpected, adverse impact. Risk management aims to gain effectiveness, minimize losses, and ensure the company stays alive with continuous development. The risk management process includes risk identification, risk analysis, risk control, and risk management evaluation and improvement.

ISO 27001 Implementation Process Steps and Approaches Organizations Use during a Cyber Attack

About the existence of actions during a cyber-attack raises the following answers from the sources. from the results of the research there are several comparisons between companies that apply or implement ISO 27001 and companies that do not. The results differ from Company 3 which does not have any security measures during a cyberattack,

due to the belief that internet firewalls and antivirus software are absolute protection, all other IT professionals stated that they have procedures in place in case a cyberattack occurs. In Company 1, the measures reflect the decision to shut down the Internet server because all company data is stored in that place. Also, if employees at this organization noticed any strange cyber activity, they would notify their IT professionals. This action is different in Companies 2, 4, and 6 where in the event of a cyberattack, IT professionals shut down Internet access.

The situation is slightly different in Company 2 where employees, if they cannot find their IT professional, have the right to shut down their computer by pressing the power button longer than usual. However, IT professionals from Company 5 seem to be the most cautious in organizing actions against the occurrence of cyberattacks. Brenner (2007) lays a foundational understanding of ISO 27001, emphasizing its importance in managing risks and achieving compliance in information security management systems (ISMS). This is further supported by Hsu, Wang, and Lu (2016), who explore the tangible impact of ISO 27001 certification on firm performance, showing a positive correlation between certification and enhanced business outcomes. Jevelin and Faza (2023) contribute a detailed evaluation of ISMS and the steps towards ISO 27001 certification, highlighting the path organizations take to achieve compliance and the benefits they experience thereafter. The study by Laghnimi et al. (2024) adds a regional perspective, specifically examining the trends and challenges in Moroccan companies, offering valuable insights for businesses in emerging markets. Olaniyi et al. (2024) addresses the strategic integration of ISO 27001 with broader cybersecurity protocols, reflecting the growing importance of digital security in today's interconnected business ecosystem. On the financial side, Sharma, and Dash (2012) provide an analytical study of the financial implications of ISO 27001 certification, while Todström (2024) presents a qualitative study of the changes experienced by small-to-medium-sized organizations in Sweden post-certification. Finally, Ukidve, Mantha, and Reddy (2022) explore the alignment of ISO 27001 controls with enterprise risk management, contributing to a deeper understanding of the certification's role in enterprise-wide risk strategies. Collectively, these articles offer a multi-faceted view of ISO 27001, making the collection an invaluable resource for both practitioners and researchers interested in information security and risk management.

In the event of such an occurrence, IT professional 5 first turns off the Internet and secondly the Internet server. He explained that the Internet server also needs to be shut down because he does not know if any viruses or malware have been placed on the system. The dominant theme in this phase is PTC which indicates that most IT professionals have created organizational cybersecurity measures that will be used in the event of cybersecurity. From the above highlights the importance of implementing cybersecurity standards, such as ISO 27001, in organizations to improve cybersecurity awareness and practices. Emphasizes that ISO 27001-certified organizations tend to have a higher level of preparedness in managing cybersecurity risks. This chapter also provides an overview of the implementation of cybersecurity standards, cooperation between management and IT staff, and efforts to improve cybersecurity awareness and practices in ISO 27001-certified organizations.

The Importance of Organizational Awareness of Information Management Security with ISO 27001 Standard

The importance of awareness of risk management as a protection of personal

data and information security, especially in today's digital era which is developing every time. The need to increase awareness in an organization along with implementing risk management at various levels, both state and federal. as a security and privacy protector for citizens.

To understand cybersecurity risk management practices and insights from ISO-certified organizations, we can look at implementation of policies and procedures in accordance with ISO/IEC 27001:2013 and ISO/IEC 27701:2019 standards. ISO-certified organizations usually have policies that ensure operational security, risk management, and compliance with established security and privacy standards. ISO-certified organizations have a better understanding of data protection and sensitive information. They adopt security and privacy design principles by default and have procedures in place to ensure third-party service providers adhere to the same security standards. Nonetheless, it is still important to evaluate and improve cyber security practices as technology and threats evolve. Before that, it is important to know that risk management in an organizational context ensures efficient identification, assessment, and management of risks related to personal information. In the research on ISO/IEC 27701:2019 and GDPR compliance models, understanding the organizational context, stakeholder needs, and expectations is key to strong compliance with global data protection regulations.

In the document presented, there is a description of cyber security risk management practices and insights from ISO certified organizations to the organization. The document shows that almost all states and the United States have weak security laws compared to the IO/IEC 270001 standard. And we can see that this is also a form of lack of awareness of the importance of risk management. It also indicates the need for better security measures to protect information after a security breach. The document also notes that laws in the United States generally do not require organizations to ensure the third parties they engage are properly verified and can guarantee an adequate level of protection. Therefore, recommendations in the document include the implementation of secure policies, effective business resilience management, and procurement and development of systems with security principles, to improve the level of data security and privacy.

CONCLUSION

The implementation of ISO 27001 in various contexts, including organizations that have obtained ISO 27001 certification and educational environments, helps improve organizational awareness of information security, operational efficiency, reduce costs due to security incidents, improve corporate reputation, protect information assets, and ensure secure operations. Thus, the application of the ISO 27001 standard in cybersecurity risk management in various sectors can provide significant benefits to organizations.

The benefits of obtaining ISO 27001 certification include substantial economic and reputational benefits. This certification helps reduce economic and reputational losses due to security attacks, and provides confidence to clients, business partners, customers, and shareholders that protective measures have been taken to safeguard the organization's assets in the case of a security attack. ISO 27001 certification can also improve an organization's overall structure, help avoid regulatory fines, and reduce the need for frequent audits.

The implementation of cybersecurity standards, such as ISO 27001, in

organizations can improve cybersecurity awareness and practices. Organizations that are ISO 27001 certified tend to have a higher level of preparedness in managing cybersecurity risks. Organizational awareness of information security with the ISO 27001 standard is important to protect personal data and information, especially in today's digital era. Data security should not be ignored in today's business context. Data protection is becoming a top priority for every organization given the increasing complexity of cyber threats. Data security strategies such as encryption, authentication.

REFERENCES

Al-Mayahi I. M. Sp (2012). Analisis GAP ISO 27001-Studi Kasus, Konferensi Internasional tentang Keamanan dan Manajemen (SAM 12), Las Vegas.

Al-Mayahi, I., & Sa'ad, P. M. (2012). Iso 27001 gap analysis-case study. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Behnia A., Rashid RA, dan Chaudhry J.A (2012, Februari). Survei Metode Analisis Risiko Keamanan Informasi, Smart Computing Review, vol. 2, no. 1.

Brenner, J. (2007). ISO 27001 risk management and compliance. *Risk management*, *54*(1), 24-29.

Ghazouani M., Medromi H., Sayouti A. (2014, April). Benhadou S., Penggunaan Terpadu ISO27005 Mehari dan Sistem Multi-Agent untuk Merancang Alat Manajemen Risiko Keamanan Informasi yang Komprehensif, International Journal of Applied Information System (IJAIS), Volume 7 - No. 2, Foundation of Computer Science, New York, Amerika Serikat, www.ijais.org.

Hsu, C., Wang, T., & Lu, A. (2016, January). The impact of ISO 27001 certification on firm performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848). IEEE.

Iskandar, Syamsul. (2013). Bank dan Lembaga Keuangan Lainnya. Jakarta: IN MEDIA.

Jevelin, J., & Faza, A. (2023). Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification. *Journal of Information Systems and Informatics*, *5*(4), 1240-1256.

Junaid, T. S. (2023). *ISO 27001: information security management systems* (Doctoral dissertation, Ph. D. thesis, Unspecified Institution. https://doi. org/10.13140/RG. 2.2. 36267.52005).

Kasmir, S. E. (2018). Bank dan lembaga keuangan lainnya edisi revisi.

Latumaerissa, J. R. (2011). Bank dan Lembaga keuangan lain.

Lembaga Standar Inggris. ISO/IEC 27001:2013 (2013). Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan. Swiss. BSI Standard Limited.

Laghnimi, J., Moumane, K., Ahmed, Z., Lamkimel, M., Kacimi, Z., & Wahi, Y. (2024, November). ISO/IEC 27001 Certification in Moroccan Companies: Trends and Future Recommendations. In *2024 World Conference on Complex Systems (WCCS)* (pp. 1-6). IEEE.

Liao, K. H., & Chueh, H. E. (2012). Medical Organization Information Security Management Based on ISO27001 Information Security Standard. *J. Softw.*, *7*(4), 792-797.

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024).

Cyberfusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 31-49.

PT. Bank Rakyat Indonesia (Persero), Tbk. (2015). Sales Kit BRI April 2015. Jakarta: Bank Rakyat Indonesia.

Sharma, N. K., & Dash, P. K. (2012). Effectiveness of ISO 27001, as an information security management system: an analytical study of financial aspects. *Far East Journal of Psychology and Business*, *9*(3), 42-55.

Todström, S. (2024). The effects of ISO 27001 certification: An interview study investigating what changes have small to medium-sized organizations in Sweden experienced after an ISO 27001 certification.

Ukidve, A., Mantha, S. S., & Reddy, D. N. (2022). Analyzing Mapping of ISO 27001: 2013 Controls for Alignment with Enterprise Risks Management. *Asian Journal of Organic & Medicinal Chemistry*, *7*(2), 123-129.

Zec, M. (2015). Cyber security Measures in SME's: a study of IT professionals' organizational cyber security awareness. *Linnaeus University, Kalmar. Zugriff unter http://www. divaportal. org/smash/get/diva2*, *849211*.