Assessing Information Security Readiness in Indonesian Fintech Companies Using KAMI Index 5.0 Framework

Merryana Lestari*[1], Maria Entina Puspita[2], Yemima Monica Geasela[3], Agustinus Fritz Wijaya[4], Puguh Hiskiawan[5], Vicky[6]
[*1,3,6] Information Systems, Universitas Bunda Mulia, Tangerang, Indonesia
[2] Accounting, STIE "AMA" Salatiga, Indonesia
[4] Informatics, Universitas Bunda Mulia, Tangerang, Indonesia
[5] Data Science, Universitas Bunda Mulia, Jakarta, Indonesia
Email: [*1]mlestari@bundamulia.ac.id, [2]mariaentina@stieama.ac.id, [3]ygeasela@bundamulia.ac.id, [4]agustinus.wijaya@bundamulia.ac.id, [5]phiskiawan@bundamulia.ac.id, [6]31220073@student.ubm.ac.id

Abstract

The development of Indonesian financial technology (fintech) has transformed the financial industry paradigm but has also introduced significant information security risks, particularly for technology-based companies. The fintech companies should establish IT governance through an Information Security Management System (ISMS) that adheres to international standards, ensuring the confidentiality, integrity, and availability of information. This work adopts a qualitative approach, deploying observations, interviews, and literature reviews on Indonesian fintech companies, especially in the digital banking fields, payment gateways, and digital wallet platforms. This study is to identify information security risks and assess the readiness and feasibility of implementing ISO/IEC 27001:2022 using the KAMI Index 5.0, which evaluates domains such as policy, governance, risk management, access control, incident management, asset management, and personal data protection. The research findings indicate that the electronic system of fintech companies plays a strategic role in supporting sustainability and business growth, with an implementation score of 809 and a fairly good level of information security feasibility. In conclusion, this reflects the company's readiness for further information security implementation. The system not only supports basic operations but also serves as a key element in achieving business objectives, both internally and externally, including regulators, banking partners, and customers.

Keywords— Financial Technology, KAMI index, ISO/IEC 27001, Information Security Management System (ISMS), IT Governance

1. INTRODUCTION

The Indonesian Fintech Development has become a phenomenon changing the financial industry, either in methods or paradigms. Since the early 2010s, the growth of the Indonesian digital economy has rapidly developed and has provided a boost for innovation, particularly in the fintech sector. Fintech is an innovation in the financial sector that allows financial transactions to be conducted more effectively, efficiently, and conveniently [1][2]. A strong internet penetration rate and rapid growth in smartphone users have created significant opportunities for various fintech companies to meet the financial needs of the community through a wide range of services [2].

The progressive support government promotes financial technology innovation, such as the fintech ecosystem for regulation issuances, which played a crucial role in the growth of this sector [3]. The Various financial transactions supporting electronic digital technology systems

refer to fintech utilization, undertaking several issues more effectively and efficiently. Various types of commonly used digital financial technologies include digital wallets, payment gateways, and digital banks. Its use is very convenient, as it only requires a smartphone, which is always carried by most people, eliminating the need for cash and physical cards, where the technology only uses internet-based applications designed to store electronic money and facilitate transactions [4][5]. The Indonesian fintech brings many positive impacts; on the other hand, there are negative impacts concerning regulators and consumers. One of the negative impacts that has become a major risk factor is the issue of information security and data privacy protections [6][7][8].

The risk of information security, especially in companies based on information technology, is quite significant [9]. Therefore, the companies need to describe to the risks related to information security by IT Governance implementing in the form of an Information Security Management System (ISMS) which designed according to international standards that can ensure the confidentiality, integrity, and availability of information by applying a more effective and efficient risk management process to identify the information security implemented in the companies [7][10][11].

However, previous studies on ISMS implementation in fintech companies have largely focused only on general frameworks and guidelines without systematically evaluating the readiness levels of these companies using structured and standardized assessment tools. There is a lack of research that specifically measures the preparedness and feasibility of fintech companies to implement ISO/IEC 27001:2022 certification through comprehensive readiness assessments, such as the KAMI Index 5.0. This gap limits understanding of how well fintech companies can adopt international information security standards and what specific areas require improvement before certification. Therefore, a prior evaluation process using the KAMI Index 5.0 is necessary to determine whether the fintech company is ready and eligible to undergo the ISO/IEC 27001:2022 information security certification, among others. Generally, fintech companies use electronic systems to run their business processes, and the KAMI Index 5.0 is commonly used to assess the readiness and feasibility of the information security used in those companies [12][13].

This research was conducted using a qualitative approach by applying observation, interviews, and literature review methods on several fintech companies in Indonesia, specifically in digital banking, payment gateways, and digital wallets. The aim was to identify risks related to information security, particularly in fintech companies in Indonesia, measure the level of readiness and feasibility of information security using the KAMI Index 5.0 in preparation for implementing ISO/IEC 27001:2022 [14]. The results of this research will provide an overview of the extent to which fintech companies in Indonesia are ready and feasible in implementing an Information Security Management System, and what recommendations should be made in the control process.

2. RESEARCH METHODS

The Information Security Index KAMI 5.0 is used as an evaluation criterion to measure the readiness, maturity level, and completeness of information security and compliance with the ISO/IEC 27001:2022 standards. The need for information security compliance regulations in fintech companies can be addressed before undergoing the assessment process. The KAMI Index is one of the structured framework tools used to assess the feasibility and readiness for data security implementation [15]. KAMI Index evaluates multiple domains, including policy, governance, risk management, access control, incident management, asset management, and personal data protection. By mapping the gap analysis results onto the KAMI Index, the researchers were able to quantify each company's current security posture and maturity level, ranging from initial (Level I) to optimal (Level V). This assessment provided a clear, standardized measure of how prepared the companies were to implement ISO/IEC 27001:2022. The results of the KAMI Index assessment become one of the valid evaluation tools used to assess the security of electronic systems and information security. The evaluation process was carried out through

interviews process on topics related to fintech, such as the categories of electronic systems used, information security governance, information security risk management, information security frameworks, information asset management, technology, personal data protection, and several information security supplements regarding third parties.

Through the interview process, the development of the fintech electronic system, which is one of the subjects of this research, was also discussed, including the OWASP Top 10 standard, which is one of the standards for evaluating information security in the development of an electronic system. This standard includes a list of 10 (ten) security vulnerabilities based on exploitability, general prevalence, detectability, and impact [16][17]. The main purpose of KAMI Index 5.0 is to evaluate the fintech company's readiness and maturity level for ISO/IEC 27001:2022 information security certification with respect to "Information Security, Cybersecurity and Privacy Protection – Information Security Management System".

The evaluation phases in the KAMI Index 5.0 are divided into two categories: readiness status assessment (Figure 1) and maturity level assessment in the implementation of security measures (Figure 2). This maturity level is used as a tool to report the mapping and assessment of information security readiness, which is defined into 5 levels: maturity level I describes the initial condition where the company is not yet mature enough to implement information security, maturity level II describes the company has only reached the implementation of the basic framework, maturity level III describes the company has a defined and consistent maturity, maturity level IV describes the company has well-managed and measurable maturity, and maturity level V describes the company has optimal maturity.

ELECTRONIC SYSTEM CATEGORIES				
Low		Final Score		Readiness Status
10	15	0	247	Not Feasible
		248	443	Need Improvement (Fullfilment of Basic Framework)
		444	760	Quite Good
		761	916	Good
High		Final Score		Readiness Status
16	34	0	387	Not Feasible
		388	646	Need Improvement (Fullfilment of Basic Framework)
		647	828	Quite Good
		829	916	Good
Strategic		Final Score		Readiness Status
35	50	0	427	Not Feasible
		473	760	Need Improvement (Fullfilment of Basic Framework)
		761	864	Quite Good
		865	916	Good

Figure 1. Correlation of Electronic System Categories with Readiness Status

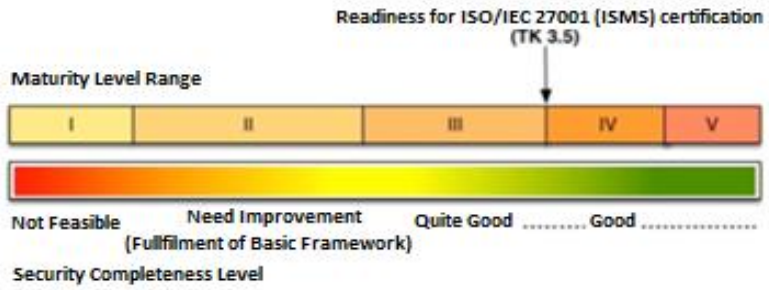

Figure 2. Range of Maturity Levels of the KAMI Index 5.0

ISO/IEC 27001:2022 is one of the internationally recognized frameworks for information security management, aimed at evaluating and improving data security to ensure that companies have an effective and reliable security system. Its implementation encompasses three main aspects: confidentiality, integrity, and availability [18][19]. The aspect of confidentiality refers to

efforts made to ensure that the data stored within the company remains protected and can only be accessed by individuals who are authorized to access it. The aspect of integrity is a principle that guarantees that the data stored, processed, and used within the company remains accurate, undisturbed, and unmodified by unauthorized parties. The aspect of availability is a process that ensures that the data stored within the company is always available and can be accessed according to the business needs of the company [20][21]. By mapping several standards related to ISO/IEC 27001:2022 with the KAMI Index, a correlation will be obtained regarding the level of readiness of the company in implementing the Information Security Management System. Through the evaluation process, improvement recommendations will be provided, which will later be used as a basis for controlling the planning and implementation process of the company's information security management [22].

The implementation method used in this research is the Plan – Do – Check – Act (PDCA) method because it is a proven, valid method in the process of implementing an Information Security Management System in a company [23]. The PDCA method consists of 1 cycle that includes 4 stages, namely the Plan stage, where the planning process is made based on recommendations from the evaluation to improve the company's information security management system. the Do stage, the process where recommendations from the evaluation are executed and implemented as a reference for the improvement of the company's information security management system. the Check stage, used as a phase in collecting or obtaining information related to the company's information security management system. Meanwhile, the Act stage is an evaluation of the implementation of the company's information security management system.

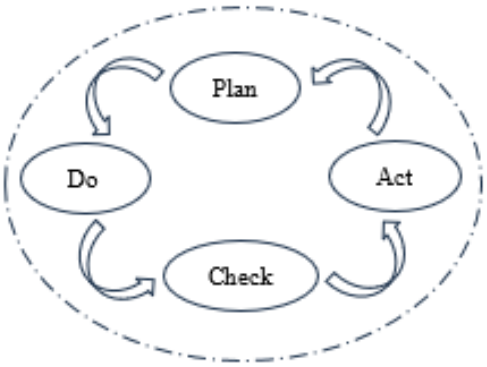

Figure 3. Plan Do Check Act Method for Implementation Planning

The PDCA method in Figure 3 is believed to be one of the practical models for continuous improvement processes for an organization. The PDCA method can be initiated at any initial stage, but it is generally started from the Plan stage, which is the planning stage, or from the Act stage, which is the evaluation process, and the cycle begins again for further improvement following the flow depicted by the PDCA method [24]. The findings at the Act stage can provide useful information for practitioners looking for ways to improve their organization's performance at the planning stage.

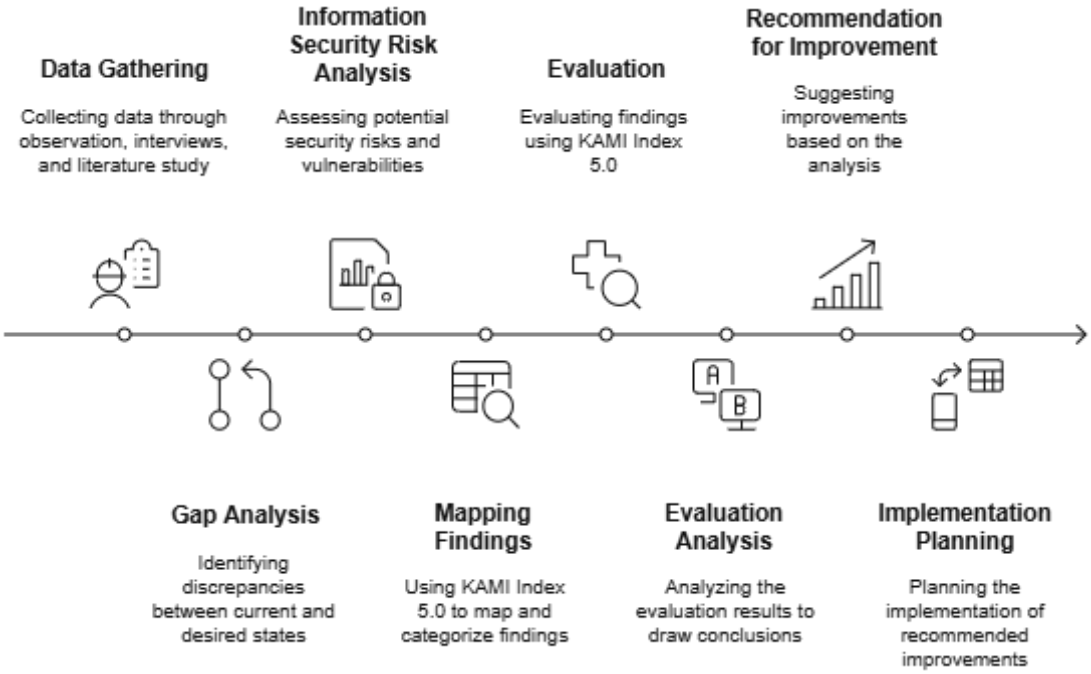

Figure 4. Research Stages in Assessing ISO/IEC 27001:2022 Implementation Readiness

The stages in this research are carried out in several phases. Initially, problem identification was conducted through data gathering involving observations, interviews, and literature study. The study focused on a single fintech company operating in Indonesia, selected based on the following criteria: active operation in the fintech sector (digital banking, payment gateways, or digital wallets), willingness to participate in the study, and having implemented or planning to implement information security management systems. Although the sample size is limited to one organization, this case study approach allows for an in-depth qualitative analysis of the company's information security readiness and maturity. Data gathering was conducted through a combination of qualitative methods to ensure a comprehensive understanding of the information security practices within the fintech companies. Semi-structured interviews were held with key personnel responsible for IT management, security, and compliance to gather in-depth insights on policies, risk management, and operational controls. Direct observations of the company's electronic systems and security protocols were carried out to verify the practical implementation of stated policies. Additionally, documentation reviews were performed on existing security policies, procedures, and compliance reports to validate and supplement the interview and observation data. This triangulation of data sources helped to ensure the reliability and completeness of the collected information. Following data gathering, a gap analysis was performed to identify findings between current practices and information security standards. The collected data were systematically processed by categorizing the current information security practices against the requirements of the ISO/IEC 27001:2022 standard. The analysis revealed areas where policies were either incomplete or inconsistently applied, weaknesses in risk management processes, insufficient access control mechanisms, and gaps in incident management and personal data protection. Next, A specific risk analysis related to information security was conducted, which evaluates domains such as policy, governance, risk management, access control, incident management, asset management, and personal data protection, with the results mapped to the KAMI Index 5.0 framework. Subsequently, an evaluation process was carried out to assess readiness and feasibility. Based on this mapping and evaluation, tailored improvement recommendations were developed and communicated to the fintech companies. These recommendations form the basis for planning the implementation of enhancements as part of the preparation for information security certification, including ISO/IEC 27001:2022, with a particular focus on aspects related to information security as seen in Figure 4.

3. RESULT AND DISCUSSION

The electronic system category determination score is used to evaluate the readiness level of the electronic system in use, with three evaluation criteria: low level, high level, and strategic level, as shown in Figure 5.

Readiness Assessment Indicator	Implementation Score	Readiness Status		
Determination Category of Electronic Systems Score	38	Strategic		
Maturity Level Assessment Indicator	**Implementation Score**	**Maturity Level**	**Final Score**	**Feasibility Status**
Governance Evaluation Score	114	Level III+	809	Quite Good
Information Security Risk Management Evaluation Score	66	Level III+		
Framework Evaluation Score	174	Level III+		
Asset Management Evaluation Score	191	Level II		
Technology and Information Security Evaluation Score	180	Level III+		
Personal Data Protection Evaluation Score	84	Level III		
Supplementary Assessment Indicator (Third-Party Security Readiness)	Implementation Score			
Evaluation of Security Involvement of Third-Party Service Providers Score	93%			

Figure 5. Results of the KAMI Index 5.0 Evaluation on Indonesian Fintech Companies

Based on the evaluation results from the research, the fintech company's electronic system received a score of 38, placing it at a strategic level. It can be concluded that the fintech company's electronic system is not only used for basic operations in business processes but also plays a strategic role in ensuring the company's sustainability, efficiency, and growth in the future. The fintech company's electronic system becomes a crucial element in supporting the company's business objectives, both internally and externally, related to third parties such as regulators, banking partners, and customers who are users of the fintech electronic system. This fintech electronic system complies with government regulations, such as legislation, and possesses licenses and guarantees from domestic and foreign banking institutions, as well as high scalability and integration with other electronic systems.

The maturity level assessment indicator for fintech companies received a final implementation score of 809, with a fairly good evaluation criterion, indicating that the company is sufficiently qualified to undergo information security certification. The assessment is divided into 6 evaluation categories, namely governance evaluation, which received an implementation score of 114, valid for maturity level III+. The symbol + indicates that the fintech company already has a defined and consistent governance maturity level III, but has not yet fully reached level IV. The evaluation of information security management received an implementation score of 66, the framework evaluation received an implementation score of 174, and the evaluation of technology and information security received a score of 180, all of which are valid for achieving a maturity level of III+. These scores indicate that the fintech company has not yet attained level IV, but it already possesses a well-defined, consistent framework, and it already has maturity in managing information security technology. Asset management evaluation, the fintech company received a valid implementation score of 191 for maturity level II, which means it has met the requirements for implementing the basic framework. Regarding the assessment of personal data protection, it received a valid implementation score of 84 for maturity level III, indicating that it is clearly defined and continuously conforms with the laws and rules pertaining to personal data protection set forth by the government and banking partner organizations.

The security readiness indicator for third-party involvement in fintech companies received an implementation score of 93%, which means the company is ready and has prepared its partners in terms of completeness, compliance, consistency, and effectiveness of the security

mechanism implementation related to risk and control, including operational services from external parties such as regulators and partners.

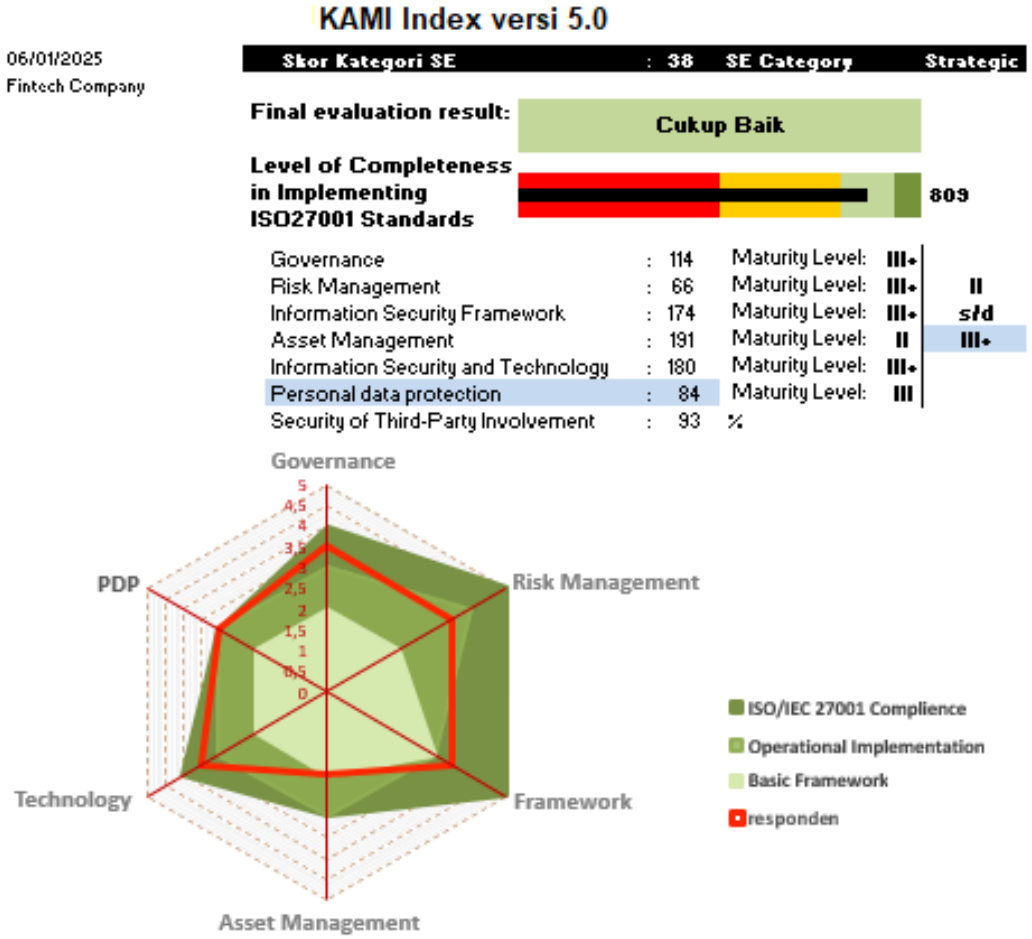

Figure 6. Evaluation Results of Indonesian fintech's Information Security Feasibility and Readiness

According to the final evaluation of the data security situation of fintech companies in Indonesia, in Figure 6, it was discovered that the condition of electronic systems in fintech firms is currently at a critical stage, with a reasonably good feasibility level for performing data security certification. Drawing from insights gained through interviews and observations, several recommendations should be put forward to enhance data security in fintech firms. These involve ensuring that all data protection policies are thoroughly recorded, effectively communicated, successfully socialized, and regularly updated to maintain relevance and adherence to best practices. Incorporating access control, monitoring, logging, risk management, and oversight of security incidents is essential, along with creating detailed evaluation metrics to ensure all aspects are regularly assessed and documented. Additionally, implementing a well-defined Service Level Agreement (SLA) for issue resolution, utilizing a ticket management system, and performing analytical security assessments can aid in tackling data breach vulnerabilities and prevent future violations. Additional recommendations include enhancing employee training programs to increase awareness and skills in cybersecurity practices, integrating digital security monitoring tools to detect and respond to threats in real time, and establishing more robust collaboration mechanisms with third-party partners and regulators to ensure comprehensive security coverage across the fintech ecosystem. Additionally, fintech firms should adopt a continuous improvement strategy by consistently revisiting and enhancing their Information Security Management System (ISMS) in line with evolving standards such as ISO/IEC 27001:2022 and emerging cybersecurity threats. These actions will strengthen the overall security stance and support economic growth in the competitive fintech environment.

4. CONCLUSION

The results of the study indicate that fintech companies' electronic systems are crucial to their long-term viability and expansion. With a score of 38, this system not only supports basic operations but also serves as a crucial element in achieving business objectives both internally and externally, including third parties such as regulators, banking partners, and customers. The electronic system of the fintech company has also complied with government regulations and possesses licenses and guarantees from banking institutions, both domestic and international, with high scalability and integration capabilities. In terms of management maturity, the fintech company achieved an implementation score of 809, indicating a "fair" criterion, which suggests that the company is ready for information security certification. The assessment of the six evaluation categories shows that corporate governance, information security management, framework, and information security technology are also at maturity level III+. Meanwhile, asset management is at maturity level II, indicating that the company still needs to strengthen the basic framework that has been implemented, while personal data protection is at maturity level III, demonstrating a good understanding, consistency, and compliance with applicable personal data protection regulations. Additionally, the readiness of third-party security received a score of 93%, indicating the company's preparedness in ensuring compliance and the effectiveness of security mechanisms applied to partners and external parties such as regulators. Thus, it can be concluded that the fintech company has achieved a good level of maturity in managing various aspects of regulatory compliance, information security, operations, and electronic system management. This study has several limitations in fintech companies, especially the ISMS readiness of the ISO/IEC 27001:2022 certification.

For future research, it is recommended to conduct a more thorough investigation of the elements affecting the attainment of maturity levels in the electronic systems of fintech companies, especially those pertaining to asset management and personal data protection. Further research can also examine how fintech companies can enhance the integration of their electronic systems with external parties, such as regulators and banking partners, to achieve a higher level of maturity. Furthermore, along with the development of increasingly complex cyber threats, research needs to expand its focus on evaluating the readiness of companies to face potential risks and dynamic regulatory changes. Further research is expected to provide insights into the obstacles faced by fintech companies in achieving Level IV maturity, as well as identifying strategies that can be implemented to accelerate its attainment and ensure the sustainability of more efficient and secure electronic systems.

REFERENCES

[1] A. G. Darmawan, M. Abdullah, K. Z. Firdausi, E. Anggraeni, and Y. Amrozi, “Financial Technology dan Masa Depan Model Transaksi Keuangan Global,” *J. Teknol. Inf.*, vol. 7, no. 2, pp. 233–238, Dec. 2023, doi: 10.36294/jurti.v7i2.3810.

[2] V. Vincent and I. N. Agustin, “Pengaruh Fintech Terhadap Kinerja Keuangan Perbankan,” *Equilib. J. Penelit. Pendidik. dan Ekon.*, vol. 21, no. 1, pp. 22–33, 2024, doi: https://doi.org/10.25134/equi.v21i01.8865.

[3] R. Marginingsih, “Financial Technology (Fintech) Dalam Inklusi Keuangan Nasional di Masa Pandemi Covid-19,” *Monet. - J. Akunt. dan Keuang.*, vol. 8, no. 1, pp. 56–64, 2021, doi: 10.31294/moneter.v8i1.9903.

[4] I. C. Santoso, A. S. Kembau, and J. Sutrisno, “‘Mengapa Pengguna Memilih Dompet Digital GoPay? Studi Tentang Pengaruh Persepsi Terhadap Kemudahan, Keamanan, Dan Manfaatnya,’” *J. Digismantech*, vol. 4, no. 1, pp. 72–87, 2024, [Online]. Available: https://journal.ubm.ac.id/index.php/digismantech/article/view/5937

[5] A. Tarigan, J. Sadeli, and H. Agung, “Uang Digital Seluler Di Era Digital Studi Kasus :

T-Cash Telkomsel Jabotabek Jabar," *J. Digismantech*, vol. 1, no. 2, pp. 57–71, 2021, [Online]. Available: https://journal.ubm.ac.id/index.php/digismantech/article/view/3626

[6] F. Kwarto and M. Angsito, "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan," *J. Akunt. Bisnis*, vol. 11, no. 2, pp. 99–110, 2018, doi: http://dx.doi.org/10.30813/jab.v11i2.1382.

[7] J. F. Andry *et al.*, "Kebijakan Keamanan Teknologi Informasi Pada Perangkat Keras Di Perusahaan Distributor Sepatu," *J. Pengabdi. dan Kewirausahaan*, vol. 7, no. 2, pp. 118–133, 2023, doi: http://dx.doi.org/10.30813/jpk.v7i2.4775.

[8] S. Meitarice, L. Febyana, A. Fitriansyah, and R. Kurniawan, "Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia : Implementation of ISO / IEC 27005 : 2018 and ISO / IEC 27001 : 2013 Security Controls," vol. 2, no. July, pp. 58–75, 2024, doi: https://doi.org/10.30996/jitcs.12099.

[9] H. Tannady, M. Fauzi Isputrawan, K. Tjandra, M. Nicholas, and J. Fernandes Andry, "Analisis Keamanan Informasi Terhadap Bencana Alam di Lab Komputer SMA XYZ Analysis of Information Security Against Natural Disasters in XYZ High School Computer Lab," *J. Bus. Audit Inf. Syst.*, vol. 6, no. 2, pp. 1–15, 2023, doi: http://dx.doi.org/10.30813/jbase.v6i2.4670.

[10] L. Hernandez, A. Pranolo, and A. P. Wibawa, "Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution," *Trans. Energy Syst. Eng. Appl.*, vol. 5, no. 2, 2024, doi: 10.32397/tesea.vol5.n2.635.

[11] C. Condolo, S. Romero, and W. Ticona, "Implementation of an Information Security Management System to Improve the IT Security of an Agricultural Tool Manufacturing Company," *Proc. 14th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu. 2024*, no. October, pp. 177–183, 2024, doi: 10.1109/Confluence60223.2024.10463232.

[12] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022," *J. SAINTEKOM*, vol. 14, no. 1, pp. 84–94, 2024, doi: 10.33020/saintekom.v14i1.623.

[13] I. P. Noven Hartawan, M. Sudarma, and I. M. . Widyantara, "[Previous Research 16 ISO 27001] [2021] ISMS Evaluation Using KAMI Index v4 Based on ISO/IEC 27001 2013 (Case Study Koperasi XYZ)," *Int. J. Eng. Emerg. Technol.*, vol. 6, no. 2, pp. 113–116, 2021, [Online]. Available: http://irjaes.com/wp-content/uploads/2021/07/IRJAES-V6N3P45Y21.pdf

[14] A. S. Anas, I. G. A. S. D. G. Utami, A. B. Maulachela, and A. Juliansyah, "KAMI index as an evaluation of academic information system security at XYZ university," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 11, no. 2, pp. 55–62, 2021, doi: http://dx.doi.org/10.31940/matrix.v11i2.2447.

[15] J. Jevelin and A. Faza, "Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification," *J. Inf. Syst. Informatics*, vol. 5, no. 4, pp. 1240–1256, 2023, doi: 10.51519/journalisi.v5i4.572.

[16] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.

[17] R. R. Yusuf and T. N. Suharsono, "Pengujian Keamanan Dengan Metode Owasp Top 10 Pada Website Eform Helpdesk," *Pros. Semin. Sos. Polit. Bisnis, Akunt. dan Tek.*, vol. 5, p. 402, 2023, doi: 10.32897/sobat.2023.5.0.3132.

[18] M. Nawir, I. AP, and F. Wajidi, "INTEGRATION OF FRAMEWORK ISO 27001 AND COBIT 2019 IN SMART TOURISM INFORMATION SECURITY PT. YoY INTERNATIONAL MANAGEMENT," *J. Komput. dan Inform.*, vol. 10, no. 2, pp. 122–128, 2022, doi: 10.35508/jicon.v10i2.7985.

[19] A. I. Wijaya, D. I. Lestiani, Y. R. Damayanti, A. Ayu, P. Sugiono, and S. C. Huanggino, "Maturity Level Risk Assessment in Media Companies with ISO 27001 Framework," vol. 3, no. 1, pp. 1–18, 2024, doi: 10.26740/jdbim.v3i1.59169.

[20] M. Waruwu and A. Indrati, "[Previous Research 15 ISO 27001 & About Audit 5] IDN Media Information Security Management System Maturity Measurement Analysis Using ISO 27001 2013 and KAMI Index Version 4," *Int. Res. J. Adv. Eng. Sci.*, vol. 6, no. 3, pp. 36–40, 2021, [Online]. Available: http://irjaes.com/wp-content/uploads/2021/07/IRJAES-V6N3P45Y21.pdf

[21] A. Rafii, A. Rafii Nugroho, and N. Legowo, "Risk Assessment at it Company by Focusing on Information Security Area Using ISO 27001:2022," *Syntax Lit. J. Ilm. Indones.*, vol. 7, no. 7, p. 12, 2022, [Online]. Available: https://jurnal.syntaxliterate.co.id/index.php/syntax-literate/article/view/15349

[22] P. Sugiarto and Y. Suryanto, "Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index based on ISO 27001:2013," *Int. J. Mech. Eng.*, vol. 7, no. 2, pp. 974–5823, 2022, doi: 10.51519/journalisi.v5i4.572.

[23] H. Setiawan and S. Supriyadi, "Perbaikan Kinerja Load Lugger dengan Menggunakan Siklus Plan-Do-Check-Action," *Ind. Inov. J. Tek. Ind.*, vol. 11, no. 2, pp. 71–78, 2021, doi: 10.36040/industri.v11i2.3637.

[24] M. P. Pratik and A. D. Vivek, "Application Of Plan-Do-Check-Act Cycle For Quality And Productivity Improvement - A Review," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 5, no. I, pp. 197–201, 2017, [Online]. Available: https://www.researchgate.net/publication/318743952_Application_Of_Plan-Do-Check-Act_Cycle_For_Quality_And_Productivity_Improvement-A_Review