Bioscientist: Jurnal Ilmiah Biologi
E-ISSN 2654-4571; P-ISSN 2338-5006
Volume 12, Issue 2, December 2024; Page, 1668-1678
Email: bioscientist@undikma.ac.id

EVALUATION OF INFORMATION SECURITY AT THE RADIN INTEN II LAMPUNG METEOROLOGICAL STATION USING THE KAMI INDEX

Ardiansyah[1*], Suhendro Yusuf Irianto[2], M. Said Hasibuan[3]
[1,2,3] Institut Bisnis dan Informasi Darmajaya, Indonesia
Email: bmg_ardiansyah@yahoo.com

DOI: https://doi.org/10.33394/bioscientist.v12i2.12498
Submit: 10-07-2024; Revised: 29-07-2024; Accepted: 30-07-2024; Published: 30-12-2024

ABSTRACT: Information security is a way to protect information assets from various potential threats. BMKG is a Non-Departmental Government Institution (LPND) in Indonesia whose main duties involve carrying out government duties in the fields of meteorology, climatology and geophysics. In connection with delivering information services appropriately and precisely to stakeholders, the Radin Inten II Lampung Meteorological Station needs to carry out an independent assessment in terms of security to evaluate the information system in each work unit, with the aim of understanding the level of readiness and maturity of information security. This research aims to measure the level of information security maturity at the Radin Inten II Lampung Meteorological Station. The analysis method used in this research is using the KAMI Index version 5.0 based on the ISO/IEC 27001:2022 standard. The research results indicate that the implementation of the ISO 27001:2022 standard in the information system of the Radin Inten II Lampung Meteorological Station is considered good. The total score obtained reached 591 based on analysis and questionnaires using the KAMI Index. With this score, the Radin Inten II Lampung Meteorological Station information system is categorized at level III, which indicates that some improvements are still needed.

Keywords: information security; KAMI index; meteorological station

How to Cite: Ardiansyah, A., Irianto, S., & Hasibuan, M. (2024). Evaluation of Information Security at the Radin Inten II Lampung Meteorological Station Using the KAMI Index. *Bioscientist: Jurnal Ilmiah Biologi*, *12*(2), 1668-1678. https://doi.org/10.33394/bioscientist.v12i2.12498

INTRODUCTION

The development of information technology (IT) is advancing very rapidly every day. As a result of this development, all organizations or companies must always adapt and implement IT advances. With the increasingly rapid development of technology today, information will be processed and stored. Information is data that can be used in the decision making process. To maintain information security, efforts need to be made to pay attention to the security factors of all supporting devices, networks and other facilities that are directly or indirectly related to the information processing process (Wowor et al., 2018). Information security is a crucial aspect but sometimes receives little attention from a government, company or organization as the owner of the information. Effective implementation of Information and Communication Technology governance can have a positive impact on organizations, especially at the executive level, to achieve their strategic goals (Syahindra et al., 2022).

Threats to information highlight the need to implement information security management in every organization or institution, including public service institutions owned by the government. So it is necessary to increase preparedness and the level of vigilance regarding potential threats to information security in government agencies, especially in critical infrastructure owned by the government (Hidayat et al., 2018).

One of the efforts that can be made by the Ministry of Communication and Information to improve the quality of information security in an agency is by creating a tool to measure the level of maturity and completeness in information security, called the Information Security Index (KAMI). The KAMI Index is a tool for measuring and analyzing the level of readiness or maturity of information security in an agency (Paramita et al., 2022). The KAMI index refers to ISO 27001 which contains information security. ISO 27001 provides a framework for the use of information technology and asset management that can help an organization ensure that the information security implemented is effective. The KAMI Index evaluates information security which includes aspects of improvement, development and implementation. The data obtained from this evaluation provides an overview of the level of readiness from completeness to maturity of the information security that has been implemented. Next, the evaluation results are analyzed, making the KAMI Index a comparison tool for making improvements (Khamil et al., 2022).

The Meteorology, Climatology and Geophysics Agency, which was previously known to the public as the Meteorology and Geophysics Agency (BMG), has changed its nomenclature to BMKG based on Presidential Regulation Number 61 of 2008 (Putri et al., 2020). BMKG is a Non-Departmental Government Institution (LPND) in Indonesia whose main duties involve carrying out government duties in the fields of meteorology, climatology and geophysics. Several aspects of BMKG's responsibilities include providing services and services in these sectors (HS, 2023). Based on the Regulation of the Head of the Meteorology, Climatology and Geophysics Agency Number 6 of 2020, the Radin Inten II Lampung Meteorological Station has the task of carrying out observations, data management, information services, meteorological services and maintenance of meteorological equipment.

In connection with delivering information services appropriately and precisely to stakeholders, the Radin Inten II Lampung Meteorological Station needs to carry out an independent assessment in terms of security to evaluate the information system in each work unit, with the aim of understanding the level of readiness and maturity of information security (Gala et al., 2020). Therefore, an evaluation is needed that can measure any deficiencies or gaps in information security at the Radin Inten II Lampung Meteorological Station, as well as conducting a review of ISO 27001:2022 as a guide to see the readiness for information security management system certification. This assessment can be done using the Information Security Index (KAMI Index) (Handari et al., 2019).

The results of the KAMI index measurements can indicate the level of information security maturity at the Radin Inten II Lampung Meteorological Station which will then be evaluated and used as a reference for increasing the level of information security in the future. The information security maturity score resulting from this research will be the basis for consideration in decision making or policy making in the field of information security at the Radin Inten II Lampung Meteorological Station in the future.

METHOD

In this method section, the methods, processes and models applied in this research will be explained. The author will also review the research steps applied in assessing security systems and information technology by utilizing the information security index (KAMI) version 5.0 based on the ISO/IEC 27001:2022 standard (Hasibuan, 2024).

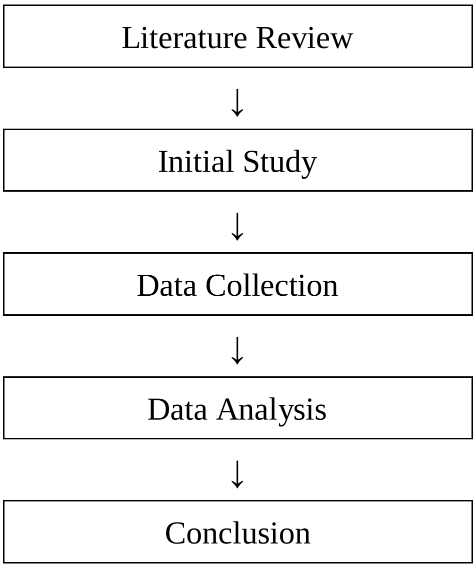


Figure 1. Research Method

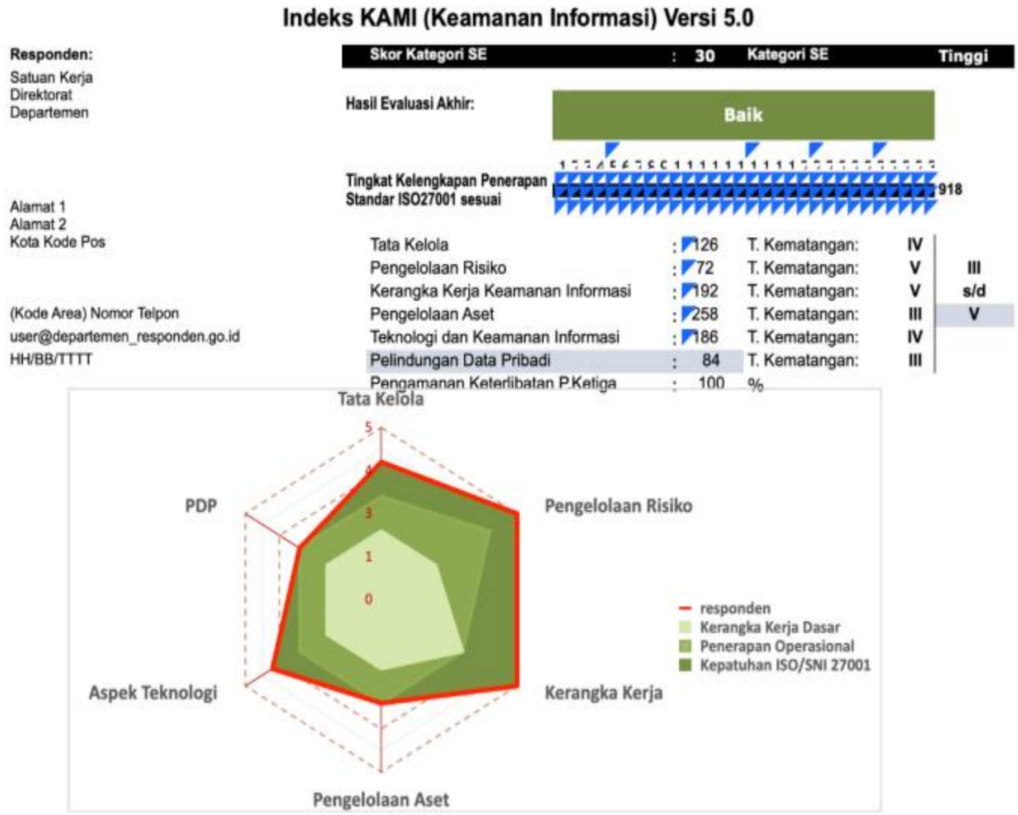
The research stages can be described as follows:

1. **Literature Study:** The initial process in this research involved a literature review with the aim of collecting data regarding the KAMI index and identifying research points that would be used as the main reference. The literature sources collected were obtained from various media, including books and journals.
2. **Preliminary Study:** The next step includes carrying out a preliminary study, which includes in-depth understanding and direct observation of the research context which is the main focus in understanding the environment in question.
3. **Data Collection:** The data acquisition process was carried out using the interview method as an information gathering technique for the head of information systems and IT staff at the Radin Inten II Lampung Meteorological Station. The main purpose of this interview is to obtain more in-depth information regarding the information system used by the station. At this stage, research involves an interaction process through interviews and data collection through filling out questionnaires based on the Information Security Index (KAMI) framework. The aim of using a questionnaire is to collect data through direct interaction with information sources.

4. **Data Analysis:** After completing the interview stage and collecting data by filling out a questionnaire based on the KAMI Index, the information that has been processed is used as a basis for analysis of problems found and preparation of suggestions for improving the performance or effectiveness of the system (Dewantara & Sugiantoro, 2021).

RESULTS AND DISCUSSION

The KAMI index is a reference tool to evaluate the level of readiness of information system security in an organization.



Indeks KAMI (Keamanan Informasi) Versi 5.0

Responden:
Satuan Kerja
Direktorat
Departemen

Alamat 1
Alamat 2
Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Skor Kategori SE : 30 Kategori SE Tinggi

Hasil Evaluasi Akhir: Baik

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai 918

Tata Kelola	:	126	T. Kematangan:	IV	
Pengelolaan Risiko	:	72	T. Kematangan:	V	III
Kerangka Kerja Keamanan Informasi	:	192	T. Kematangan:	V	s/d
Pengelolaan Aset	:	258	T. Kematangan:	III	V
Teknologi dan Keamanan Informasi	:	186	T. Kematangan:	IV	
Pelindungan Data Pribadi	:	84	T. Kematangan:	III	
Pengamanan Keterlibatan P.Ketiga	:	100	%		

Figure 2. KAMI Index Results

Analysis of Electronic System Categories

This section evaluates the level or category of electronic systems used. Electronic system category analysis helps in understanding the characteristics, needs, and challenges associated with each type of system, making it easier to develop, maintain, and optimize the system. Analysis of electronic system categories includes assessing, identifying and grouping electronic systems based on various criteria or certain characteristics. These categories can be function, complexity, application, or technology used.

The electronic system components received a score of 30, reflecting a fairly high level of technology dependence. Factors that contribute to this high score include the implementation of cryptographic techniques in accordance with standards or internal developments. Cryptography plays a major role in protecting the contents of data or messages, ensuring that only parties who have the right and authority can interpret them.

Table 1. Electronic Systems Category

Electronic Systems Category	Scores
Low	10 – 15
High	16 – 34
Strategic	35 – 50

Even though it achieves a high score, it doesn’t mean that the electronic system doesn't have weaknesses. There are several aspects that need to be improved so that the index in the electronic system can be improved. Recommendations for improvement involve increasing compliance with regulations and standards at both national and international levels.

Information Security Governance Analysis

Information security governance analysis involves evaluating and understanding how an organization manages and protects its important information from existing threats and risks. The following are several key elements in information security governance analysis:

1. Security Policies: Evaluate existing security policies, including access policies, password policies, monitoring policies, and security incident response policies. The analysis also includes the effectiveness of the policy in protecting the organization's information.
2. Information Classification: Analyze how information is classified based on its level of importance and how that affects the protection afforded to it. This includes sensitive information handling and storage policies.
3. Access Management: Evaluate how access to information is controlled and managed throughout the organization. This includes access rights management, user authentication, and user activity monitoring.
4. Technical Controls: Analysis of the technological infrastructure used to protect information, such as firewalls, antivirus, data encryption, and intrusion detection systems. It is important to evaluate the effectiveness and adequacy of these technical controls.
5. Security Awareness: Analyze the level of security awareness and training provided to employees. Good security awareness can be an important defense against cyberattacks.
6. Risk Management: Evaluation of the process of identifying, evaluating and handling information security risks. This includes an understanding of potential threats, system vulnerabilities, and the impact of security incidents.
7. Regulatory Compliance: Analyze the extent to which the organization complies with applicable security regulations and standards, such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), or PCI DSS (Payment Card Industry Data Security Standard).

This section evaluates the readiness of the agency/company's form of information security governance along with the functions, duties and responsibilities of information security managers. The governance section has a score of 126, indicating that it is currently at level IV. The most prominent element in information security management is the integration of user security at the Radin Inten II Lampung Meteorological Station. In addition, capability and expertise standards also have a significant impact on information security governance scores. Information security governance analysis helps organizations to identify weaknesses in their security strategies, improve compliance, and reduce risks associated with information leakage or misuse. Therefore, Even though it has reached level III, improvements are still needed, and within this framework, one of the proposed improvements is to implement policies aimed at dealing with information security incidents involving violations of the law.

Information Security Risk Management Analysis

Information security risk management analysis helps organizations to identify, evaluate, and manage risks associated with information security, thereby enabling them to take appropriate steps to protect valuable information assets. This section evaluates the readiness to implement information security risk management as a basis for implementing information security strategies.

The following are the main steps in information security risk management analysis:

1. Risk Identification: The process of identifying potential threats and vulnerabilities in an organization's information environment. This involves a deep understanding of information assets, as well as threats that may threaten their security and integrity.
2. Risk Evaluation: After risk identification, the next step is to evaluate the potential impact of the risk and its likelihood of occurrence. This helps in determining the level of risk that needs to be addressed and the priority of mitigation actions.
3. Risk Reduction: After evaluating the risks, the organization must take steps to reduce the identified risks. This may involve implementing additional security controls, process improvements, or employee training.
4. Risk Transfer: Some risks may be better transferred to another party, such as an insurance institution. This is done by determining risks that cannot be addressed internally and seeking external solutions to address those risks.
5. Accept the Risk: In some cases, a particular risk may be accepted by the organization because the cost or complexity of the risk reduction action is higher than the possible impact of the risk.
6. Ongoing Monitoring and Management: Information security risk management processes should be part of ongoing business practices. This includes continuous monitoring of the information security environment, periodic re-evaluation of risks, and adjustment of risk management strategies according to changes in threats or business conditions.

7. Regulatory Compliance: Ensure that information security risk management strategies comply with all applicable security regulations and standards for the relevant industry or jurisdiction.

With a score of 72 and being at level IV, the risk section has shown excellent performance. However, security still requires improvement in various sectors related to security risks. The Radin Inten II Lampung Meteorological Station information system has advantages in identifying threats to information assets, so it gets a high score in that section. There are several suggestions for improvement in the information security risk aspect, including the importance of identifying the impact of losses associated with disruption to assets. Another suggestion for improvement is to implement risk mitigation measures regularly with the aim of ensuring performance progress and effective resolution.

Information Security Management Framework Analysis

An information security management framework is a conceptual structure that provides guidelines and procedures for managing information security within an organization. This framework helps organizations to effectively identify, measure, manage and improve their information security. This section evaluates the completeness and readiness of the information security management framework (policies & procedures) and its implementation strategy. Information security management frameworks help organizations to manage information security risks in a structured and efficient manner, thereby ensuring adequate protection of their information assets.

The Radin Inten II Lampung Meteorological Station received a score of 192 and is currently at level IV in the framework elements. A very important value contribution in the information security framework is the openness of information security policies to organizational staff. In developing information systems, the Radin Inten II Lampung Meteorological Station has adopted development techniques in accordance with standard methods. However, a number of recommendations for improvement in the framework involve the need for internal audits to ensure compliance and consistency in information security management. Apart from that, carrying out routine test evaluations related to information security management is also a crucial step.

Information Asset Management Analysis

Information asset management analysis involves evaluating and understanding how an organization manages their information assets in an effective and efficient manner. This includes the processes of identifying, protecting, monitoring, and maintaining information assets that are important to the organization. This section evaluates the completeness of the security of information assets, including the entire use cycle of these assets. The following are several main components in information asset management analysis:

1. Identification of Information Assets: The first step in managing information assets is identifying the information assets owned by the organization. This can include sensitive data, documents, databases, source code, IT infrastructure, and so on.

2. Asset Value Assessment: Once information assets are identified, the next step is to assess the value of each asset. This assessment can be based on the strategic importance, sensitivity, financial value, or operational criticality of the asset.
3. Asset Protection: Organizations need to take steps to protect their information assets from existing threats and risks. This can include implementing access controls, data encryption, security monitoring, and other protective measures appropriate to the asset's value and needs.
4. Asset Maintenance: Management of information assets also involves regular maintenance and updating of those assets. This includes technical maintenance, version management, security updates, and asset performance monitoring to stay relevant and effective.
5. Asset Life Cycle Management: Every information asset has a life cycle that includes creation, use, storage, maintenance, and finally deletion. Organizations need to have a structured process to properly manage the lifecycle of these assets.
6. Monitoring and Evaluation: Management of information assets also involves continuous monitoring and evaluation of the security, availability, and integrity of those assets. This allows organizations to identify and respond quickly to possible threats or incidents.
7. Regulatory Compliance: It is important to ensure that information asset management complies with all relevant security regulations, standards and policies. This includes compliance with regulations such as GDPR, HIPAA, PCI DSS, and others that may apply to the organization.

By obtaining a score of 256, the asset management section at the Radin Inten II Lampung Meteorological Station was placed at level IV. Asset management at the Radin Inten II Lampung Meteorological Station still requires a number of improvements, although several aspects have been implemented thoroughly, such as the existence of provisions or policies for the use of email and computers within the organization. In addition, procedural policies related to data backup and deletion of assets that are no longer relevant are also significant value contributing factors. The findings' recommendations in asset management involve the need to implement a change management process for business systems and processes. On the other hand, the Radin Inten II Lampung Meteorological Station has not fully adopted a consistent change management process in asset management.

Technology and Information Security Analysis

This section evaluates the completeness, consistency and effectiveness of the use of technology in securing information assets. By getting a score of 186 in the information system security technology section, the Radin Inten II Lampung Meteorological Station is at level IV. Implementing a communication network that suits your interests is one of the factors that contributes to value in the technological aspect. The existence of network monitoring also contributes to the security quality of the information system at the Radin Inten II Lampung Meteorological Station. Even though it is at level III, the security and technology aspects still need improvement, and recommendations include the use of antivirus on desktops and servers. This is because malware can have negative impacts, such as theft of information or personal data. In addition, the research found that regular evaluation of the reliability of the security system has not been fully implemented at the Radin Inten II Lampung Meteorological Station.

Analysis of Personal Data Protection (PDP)

Personal data protection analysis involves assessing the steps taken by an organization to protect the personal data they collect, store and process. Protection of personal data is essential to ensure the privacy and security of individuals to whom that data relates. This section evaluates the completeness, consistency and effectiveness of the implementation of security controls related to Personal Data Protection (PDP). Personal data protection analysis helps organizations to evaluate the effectiveness and compliance of their security practices for personal data. This is important to ensure that individuals' personal data remains safe, secure and is not misused.

Based on data from interviews and questionnaires using the KAMI index on the Radin Inten II Lampung Meteorological Station information system, data was obtained which is presented in the form of a bar chart. The questionnaire questions consist of 7 evaluation aspects that have been adapted based on the KAMI Index framework. These seven aspects consist of evaluation of electronic systems, technology, risks, governance, frameworks, asset management, and supplements. The data obtained will be the basis for evaluating and improving the information system at the Radin Inten II Lampung Meteorological Station.

For the latest evaluation results, a score of 591 was obtained, indicating that the information system of the Radin Inten II Lampung Meteorological Station has implemented most of the principles of information system governance correctly and in accordance with what is required. However, weaknesses are still identified in several areas related to data and information security.

CONCLUSION

Research on the information system at the Radin Inten II Lampung Meteorological Station shows that the application of the ISO 27001:2022 standard to the information system at the Radin Inten II Lampung Meteorological Station is considered good. The total score obtained reached 591 based on analysis and questionnaires using the KAMI Index. With this score, the Radin Inten II Lampung Meteorological Station information system is categorized at level III, which indicates that some improvements are still needed.

ACKNOWLEDGMENT

The author expresses infinite gratitude to all parties directly involved in this research, as well as to those who contributed indirectly.

REFERENCES

Barani, G. D. S., Putra, W. H. N., & Prakoso, B. S. (2020). Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI (Keamanan Informasi) 4.0 (Studi Kasus: Dinas Komunikasi dan Informatika Provinsi Jawa Timur). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *4*(9), 3218–3224. http://j-ptiik.ub.ac.id

Dewantara, R., & Sugiantoro, B. (2021). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *8*(6), 1137–1148. https://doi.org/10.25126/jtiik.2021863123

Handari, D. C., Fakih, M., & Oktaviana, S. (2019). Analisis Perjanjian Diseminasi Informasi Iklim (Studi Pada Perjanjian Kerjasama antara Badan Meteorologi, Klimatologi dan Geofisika (BMKG) dengan Lembaga Penyiaran Publik (LPP) Televisi Republik Indonesia (TVRI Stasiun Lampung). *Pactum Law Journal*, *2*(2), 676–690.

Hidayat, R., Suyanto, M., & Fatta, H. Al. (2018). Indeks Penilaian Keamanan Informasi Untuk Mengukur Kematangan Manajemen Keamanan Layanan TI (Studi Kasus: BPMP Kabupaten Gresik). *Jurnal Informatika Dan Teknologi Informasi*, *3*(1), 27–34. http://e-journal.janabadra.ac.id/

HS, I. M. (2023). Dampak Digitisasi dan Digitalisasi Arsip Terhadap Pelayanan Publik Di Stasiun Meteorologi Kelas I Radin Inten II Lampung. *JSL: Jurnal Socia Logica*, *3*(1), 1–10.

Khamil, D. I., Sasmita, G. M. A., & Susila, A. A. N. H. (2022). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar). *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(3), 1948–1960. http://jurnal.mdp.ac.id

Kornelia, A., & Irawan, D. (2021a). Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1. *Jurnal Pengembangan Sistem Informasi Dan Informatika*, *2*(2), 78–86.

Kornelia, A., & Irawan, D. (2021b). Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1. *Jurnal Pengembangan Sistem Informasi Dan Informatika*, *2*(2), 78–86. https://doi.org/10.47747/jpsii.v2i2.548

Matondang, N., Hananto, B., & Nugrahaeni, C. (2019). Analisis Tingkat Kesiapan Pengamanan Sistem Informasi (Studi Kasus UPN Veteran Jakarta). *Jurnal Teknologi Informasi Dan Pendidikan*, *12*(1), 1–4.

Natalia, E., Hoyyi, A., & Santoso, R. (2017). Analisis Kepuasan Masyarakat Terhadap Pelayanan Publik Menggunakan Pendekatan Partial Least Square (PLS) (Studi Kasus: Badan Arsip dan Perpustakaan Daerah Provinsi Jawa Tengah). *Jurnal Gaussian*, *6*(3), 313–323. http://ejournal-s1.undip.ac.id/index.php/gaussian

Paramita, S., Siregar, S. A., Damanik, R. A., & Irawan, M. D. (2022). Bulletin of Information Technology (BIT) Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013. *Bulletin of Information Technology (BIT)*, *3*(4), 374–379. https://doi.org/10.47065/bit.v3i1

Pratiwi, H. A., & Wulandari, L. (n.d.). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor. *Journal of Industrial Engineering & Management Research*, *2*(5), 146–163. https://doi.org/10.7777/jiemar

Putri, D. F., Triwahyuni, T., Husna, I., & Sandrawati. (2020). Hubungan Faktor Suhu dan Kelembaban Dengan Kasus Demam Berdarah Dengue (DBD) di Kota Bandar Lampung. *Jurnal Analis Kesehatan*, *9*(1), 17–23.

R, K. H., & Hasibuan, M. S. (2024). Analisis Tingkat Kematangan Keamanan Informasi Menggunakan Indeks KAMI pada Tiyuh Pulung Kencana. *Journal of Digital Literacy and Volunteering*, *2*(1), 31–37. https://doi.org/10.57119/litdig.v2i1.78

Gala, R. A. P. P., Sengkey, R., & Punusingon, C. (2020). Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI. *Jurnal Teknik Informatika*, *15*(3), 189–198.

RI, K. P. (2022). *LAPORAN HASIL SURVEI KEPUASAN MASYARAKAT (SKM) PENGGUNA LAYANAN PUBLIK KEMENTERIAN PUPR*.

Syahindra, I. P. S., Primasari, C. H., & Irianto, A. B. P. (2022). Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks Kami Dan Iso 27005 : 2011. *Jurnal TEKNOINFO*, *16*(2), 165–182. https://doi.org/10.33365/jti.v16i2.1246

WIJATMOKO, T. E. (2020). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Kantor Wilayah Kementerian Hukum Dan HAM DIY. *Cyber Security Dan Forensik Digital*, *3*(1), 1–6. https://doi.org/10.14421/csecurity.2020.3.1.1951

Wijaya, Y. D. (2021). Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013. *Jurnal Sistem Informasi Dan Informatika (Simika)*, *4*(2), 115–130. https://doi.org/10.47080/simika.v4i2.1178

Wowor, N. E., Sentinuwo, S. R., & Karouw, S. D. S. (2018). Analisa Keamanan Informasi Pemerintah Kota Manado Menggunakan Indeks KAMI. *Jurnal Teknik Informatika*, *13*(3), 1–10.