VOL. 23 (2) (2026), XX-XXp-ISSN: 693-7554, e-ISSN:2654-3990

Assessment of Information Security Maturity Using the KAMI Index 5.0 Aligned with ISO/IEC 27001

Fitri Safnita[1*], **Putri Ramadani**[2], **Maisan Dewi Puspa Khairani**[3], **Eka Ramadhani Putra**[4]

[1] Département of Informatics, Faculty of Industrial Technology, Bung Hatta University, Padang, West Sumatra, Indonesia

[2] Department of Information System, Faculty of Computer Science, Ika Bina Institute of Technology and Health, North Sumatra, Indonesia

[3] Department of System Computer, Faculty of Computer Science, Pamulang University, Banten, Indonesia

[4] Department of Information System, Faculty of Computer Science, Pamulang University, Banten, Indonesia

Abstract

The advancement of digital government initiatives has led to a wider deployment of IT systems for public service delivery. Consequently, public sector agencies must establish robust cyber defenses to safeguard critical information and infrastructure. This research evaluates the information security posture of the Padang City Communication and Informatics Office, focusing on its readiness to sustain digital transformation. The assessment aligns with the ISO/IEC 27001 framework and utilizes the KAMI Index 5.0 as the primary diagnostic tool. Employing a qualitative descriptive methodology, the study collected empirical data through field observations, stakeholder interviews, and comprehensive policy reviews. The diagnostic results revealed a compliance score of 518, demonstrating that the organization has established the baseline requirements of the ISO/IEC 27001 standard. Nonetheless, the overall maturity remains at Level II, showing that while several protective processes are active, they lack formal documentation and optimal coordination. To bridge these gaps, structured action plans are formulated across seven key assessment domains: governance (5 actions), risk mitigation (14 actions), security policy framework (5 actions), asset classification (13 actions), technical infrastructure (6 actions), data privacy (11 actions), and third-party control (6 actions). These actionable steps provide a strategic roadmap to enhance the mature of city's electronic administration security.

Keywords: *Information Security; ISO/IEC 27001; KAMI Index 5.0; Digital Transformation; Information Security Governance*

1. Introduction

Effectively managing information as a strategic resource is vital for public institutions, helping to reinforce administrative capabilities and improve operational competitiveness [1]. Amid rapid digitalization, organizational data represents an invaluable yet highly targeted asset that is continuously exposed to security breaches and unauthorized intrusion [2]. The increasing use of information technology systems demands serious attention because these systems process and store critical assets, such as personal data, public records, and academic records [3]. Establishing a formalized defense framework is thus critical to shield proprietary records and preserve their fundamental confidentiality, integrity, and availability (CIA triad) [4]. In addition, because public-facing entities are designed to be accessible, they present soft targets for rising cyber exploits, including deceptive phishing schemes, system-locking ransomware, and disruptive malicious software [5].

The existence of information systems, originally designed to function as strategic tools, can turn into major threats if potential risks are not properly managed and mitigated [6]. Regrettably, inadequate cybersecurity awareness among workforce members frequently exposes administrative vulnerabilities, leading to serious operational disruptions and process failures [7]. Today's digitalization of public and educational services faces real challenges in the form of cyber threats, which require structural evaluation to safeguard services and maintain user trust [8]. Considering that the use of technology cannot escape the looming threat of incidents, organizations are required to consistently identify and protect their assets [9].

*Corresponding author. *E-mail address:* fitrisafnita@bunghatta.ac.id
Received: 10 June 2026, Accepted: 30 July 2026 and available online 31 July 2026
DOI: https://doi.org/10.33751/komputasi.v23i2.110

These security efforts must be comprehensive, encompassing the supervision of all supporting devices, network infrastructure, and facilities related to data processing activities [10]. This means that information security can no longer be viewed solely from a technical perspective, but must include the integration of policies, procedures, and the awareness of all organizational elements [11]. To minimize these loopholes, designing and implementing a structured information security management system using international standards is crucial in dealing with increasingly complex cyber threats [12]. The rapid advancement of information technology brings new challenges for institutions in ensuring their data protection aligns with global frameworks [13]. Capable information technology security governance will protect assets and ensure service continuity, which simultaneously serves as a strategic preparatory step for institutions towards ISO/IEC 27001 standardization and certification [14]. Ultimately, the implementation of security frameworks such as the ISO 27001 standard will significantly assist institutions in mitigating vulnerabilities, protecting system integrity, and rebuilding stakeholder trust [15].

In practice, to achieve these security standards, both government and private institutions must periodically evaluate their security governance to comply with applicable regulations and guarantee data security [16]. This evaluation has proven to be highly crucial, for instance, in the implementation of the Electronic-Based Government System (SPBE) in Indonesia, to prevent organizations from experiencing recurring technical security issues [17]. The routine implementation of security evaluations using official measurement tools such as the Information Security Index (Indeks KAMI) serves as a primary instrument to ensure organizational compliance with regulations while fostering a culture of security awareness among users [18]. Through the implementation of self-evaluations based on the KAMI Index, institutions can anticipate unforeseen risks that potentially paralyze their electronic systems [19]. Furthermore, with this evaluation tool, organizations can map the level, size, and degree of importance of their operational systems to subsequently formulate effective and targeted governance improvement measures [20].

2. Methods

A descriptive-evaluative case study design was selected to analyze the robustness of information defenses within the Padang municipal administration during its transition to digital systems. The audit was structured around the BSSN-developed KAMI Index (version 5.0), a standardized national assessment aligned directly with ISO/IEC 27001. Figure 1 outlines the sequential phases of the research.

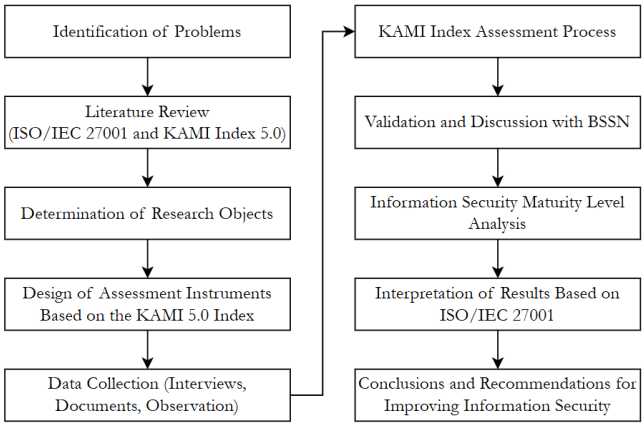

Figure 1. Methodology

The investigative flow progressed through distinct stages: defining the research problem, conducting a systematic literature synthesis, gathering empirical evidence, running the KAMI Index diagnostic, and interpreting the compiled findings. Data collection was conducted through observations, reviews of information security policy documents, and discussions with relevant stakeholders within the Communication and Informatics Office of Padang City. In this study, the researchers were directly involved in the KAMI Index 5.0 evaluation process, starting from identifying the current condition of information security, designing the assessment process, collecting data, and conducting the evaluation together with the local government team. The assessment results were then discussed and validated through an evaluation meeting with the National Cyber and Crypto Agency (BSSN) to ensure compliance with the applicable assessment standards.

Furthermore, the evaluation scores were analyzed to determine the maturity level of information security and its alignment with the ISO/IEC 27001 framework. This analysis provides an overview of the readiness of the Communication and Informatics Office of Padang City in managing information security to support digital transformation.

To evaluate maturity, the KAMI 5.0 framework uses a non-linear, tiered evaluation logic designed by BSSN, moving away from basic score averaging [21]. Individual domain questions are mapped across three progressive performance tiers: Tier 1 (baseline controls), Tier 2 (implementation consistency), and Tier 3 (ongoing audit and system optimization). Reaching advanced maturity ratings (ranging from Level I up to Level V, along with the '+' sub-tiers) demands satisfying minimum score requirements combined with strict gateway rules. Most importantly, if core baseline controls (Tier 1) are marked as pending or planned, the final

rating for that specific domain is capped at Level I or I+, even if advanced Tier 2 or 3 measures are already operational.

3. Result and Discussion

Before starting stakeholder interviews, the boundaries of the security audit were established. The scope covered all municipal data, stored information, and active transactional platforms overseen by the Padang City Communication and Informatics Office. An initial inventory check classified the operational systems to determine their administrative significance.

Table 1. Electronic System Category Assessment Data

Part I : Electronic System Category		
Total Questions		10
Respondents' Answer Results		
Answer Choices	**Result**	**Score**
[A]	3	15
[B]	6	12
[C]	1	1
Total Score for Electronic Systems Category		**28**

The baseline metrics summarized in Table 1 show an electronic system category score of 28, indicating a 'High' reliance classification. Furthermore, the results of the assessment data for the areas of information security governance, information security risk management, information security framework, asset management, technology and information security, and supplementary areas are presented in the following table.

Table 2. Governance Security Assessment

Part II: Information Security Governance			
Respondents' Answer Results			
Security Status	**Security Category**		
	SC 1	**SC 2**	**SC 3**
Are not done	0	0	0
In Planning	0	0	0
In Implementation or Partially Implemented	0	4	1
Implemented comprehensively	9	2	6
Total Governance Value		**118**	

Table 3. Risk Management Security Assessment

Part III: Risk Management			
Respondents' Answer Results			
Security Status	**Security Category**		
	SC 1	**SC 2**	**SC 3**
Are not done	0	0	0
In Planning	0	0	0
In Implementation or Partially Implemented	8	2	4
Implemented comprehensively	2	0	0
Total Risk Management Value		**38**	

Table 4. Framework Safeguard Assessment

Part IV: Framework			
Respondents' Answer Results			
Security Status	**Security Category**		
	SC 1	**SC 2**	**SC 3**
Are not done	0	3	0
In Planning	2	0	0
In Implementation or Partially Implemented	8	10	0
Implemented comprehensively	3	3	4
Total Framework Value		**70**	

Table 5. Asset Management Security Assessment

Part V: Asset Management			
Respondents' Answer Results			
Security Status	**Security Category**		
	SC 1	**SC 2**	**SC 3**
Not Applicable/Relevant	0	11	0
Are not done	0	1	0
In Planning	0	1	0
In Implementation or Partially Implemented	23	5	0
Implemented comprehensively	9	3	0
Total Asset Management Value		**161**	

Table 6. Technology and Security Assessment

Part VI: Information Technology and Security			
Respondents' Answer Results			
Security Status	**Security Category**		
	SC 1	**SC 2**	**SC 3**
Are not done	0	0	0
In Planning	4	1	1
In Implementation or Partially Implemented	8	10	2
Implemented comprehensively	5	4	0
Total Technology and Security Value		**118**	

Table 7. Personal Data Protection Assessment

Part VII: Protection of Personal Data			
Respondents' Answer Results			
Security Status	**Security Category**		
	SC 1	**SC 2**	**SC 3**
Are not done	4	7	0
In Planning	1	2	0
In Implementation or Partially Implemented	1	0	0
Implemented comprehensively	0	1	0
Total Personal Data Protection Value		**13**	

Table 8. Supplement Assessment

Part VIII: Supplements			
Respondents' Answer Results			
Security Status	**Security Category**		
	SC 1	**SC 2**	**SC 3**
Are not done	6	0	7
In Planning	0	3	9
In Implementation or Partially Implemented	1	0	1
Implemented comprehensively	0	0	0
Total Supplement Value		**16**	

Figure 2. Completeness and Security Assessment Results

Based on the results shown in Figure 2, it can be concluded that in the electronic system category, the Communication and Informatics Office of Padang City achieved a score of 28, indicating that electronic systems have become an integral part of the organization's activities and are categorized as "High." Meanwhile, the level of completeness in meeting the ISO/IEC 27001 standard, in accordance with the electronic system category, reached a total score of 518, which is classified as "Basic Framework Fulfillment".

Table 9. Percentage of Achieved Maturity Level

Information	Area 1	Area 2	Area 3	Area 4	Area 5	Area 6	Area 7
Respondent Score	118	38	70	161	118	13	16
Presentation	54%	24%	31,2%	93,6%	33,6%	19,2%	20%
Maturity Level	III+	II	II	I+	II	I	I

Based on Table 9, in Area 1 (Information Security Governance), a score of 118 was obtained with an achievement percentage of 54%, reaching a maturity level of III+. In Area 2 (Information Security Risk Management), the score obtained was 38 with an achievement percentage of 24%, reaching maturity level II. In Area 3 (Information Security Framework), the score obtained was 70 with an achievement percentage of 31.2%, reaching maturity level II. In Area 4 (Asset Management), the score obtained was 161 with an achievement percentage of 93.6%, reaching maturity level I+. In Area 5 (Technology and Information Security), the score obtained was 118 with an achievement percentage of 33.6%, reaching maturity level II. In Area 6 (Personal Data Protection), the score obtained was 13 with an achievement percentage of 19.2%, reaching maturity level I. The final area is the Supplementary Area, where the third-party security aspect obtained a score of 16 with an achievement percentage of 20%.

As shown in Table 9, a notable discrepancy occurs in Area 4 (Asset Management), which achieved the highest raw score of 161 (93.6% compliance) yet was designated at Maturity Level I+. In contrast, Area 1 (Governance) scored 118 (54% compliance) but reached Maturity Level III+. This occurs due to the progressive dependency logic built into the BSSN KAMI Index evaluation tool. In Asset Management, the organization has implemented robust technical and physical security measures, such as inventory tracking and cloud security configurations, which generated a high raw score. However, several critical, non-negotiable Stage 1 foundational policies—such as a formal information classification policy and fully documented asset return procedures—remain in the planning or partial implementation phase. Because these fundamental Stage 1 prerequisites are not completely finalized, the evaluation algorithm strictly caps the overall maturity at Level I+ to emphasize that technical implementations cannot substitute for missing core organizational policies.

Area 6 (Personal Data Protection) received the lowest score of 13 (19.2% compliance, Maturity Level I) among all assessed domains. This performance reflects a combination of structural policy gaps, limited organizational awareness, and the relative novelty of the regulatory requirements. First, BSSN integrated strict PDP compliance controls into the KAMI Index 5.0 only recently to align with the national personal data protection framework (under Government Regulation PP No. 71/2019 [23] and the PDP Law UU No. 27/2022 [22]). Consequently, local government bodies like the Communication and Informatics Office of Padang City are still in the early stages of adapting their workflows to these legal standards. Structurally, there is a lack of dedicated data privacy roles, such as a Data Protection Officer (DPO), and an absence of formal privacy impact assessments (PIA). Furthermore, internal training and awareness programs remain heavily centered around general system availability and network security rather than the specific lifecycle management and protection of personally identifiable information (PII).

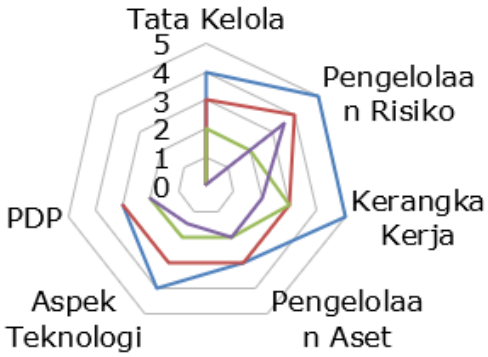

Figure 3. Completeness Level Radar Diagram

The multi-axis radar chart in Figure 3 visually represents the implementation completeness across the evaluated security domains. The visualization reveals that Information Security Governance is the most

advanced sector, achieving Maturity Level III+ (54%), which signifies that the municipal office has successfully instituted fundamental policy structures. The areas of Risk Management, Information Security Framework, and Technology and Security are moderately positioned at Level II (Basic Framework Fulfillment), indicating key processes are operational but lack robust documentation and consistent management. Meanwhile, despite showing a high raw completeness score of 93.6% (161), Asset Management remains capped at Level I+ due to missing foundational policies. The lowest achievements are recorded in Personal Data Protection (Level I) and the Supplementary area (Level I), highlighting critical vulnerabilities and a pressing need for prioritized remediation.

To contextualize these findings, a comparative analysis was performed with other structurally comparable local government bodies in Indonesia evaluated under the KAMI Index framework. For instance, the Communication and Informatics Office (Diskominfo) of Malang City previously achieved a maturity level of I+ to II [16, 17], facing similar challenges where technical tools were partially active but formal documentation and consistent risk management remained deficient. Similarly, evaluations at Diskominfo Sumedang [8] highlight that local government agencies consistently struggle to surpass Maturity Level II due to systemic bottlenecks, primarily the slow formalization of security policies. The evaluation of Diskominfo Padang City in this study aligns with this national trend, demonstrating that while basic technical defenses are operational, a formalized, documented, and risk-aware administrative framework is the main barrier preventing local public services from achieving mature information security standards (Level III+).

4. Conclusion

In conclusion, assessing the Padang City Communication and Informatics Office via the KAMI Index 5.0 indicates that the organization has established a baseline defense framework, achieving an overall score of 518. While this score demonstrates alignment with foundational ISO/IEC 27001 tenets, the overall maturity rating of Level II highlights that several active processes lack proper standardization, comprehensive documentation, and unified oversight. To address these weaknesses and elevate maturity levels, targeted action items are proposed: 5 focused on governance, 14 on risk management processes, 5 on policy framework alignment, 13 on administrative asset tracking, 6 on hardware/software technical controls, 11 on consumer data privacy measures, and 6 on third-party security management. These recommendations are expected to serve as a basis for the organization to improve the effectiveness of information security management implementation and support the sustainability of local government digital services.

For future research, it is recommended to further develop information security risk management analysis by integrating established risk management frameworks. Specifically, organizations should leverage NIST SP 800-37 (Risk Management Framework / RMF) to guide the multi-step lifecycle process of risk identification and monitoring, alongside NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) to select and implement granular, technical security controls. These publications should be used to complement, rather than replace, the BSSN KAMI Index 5.0. While the KAMI Index provides a vital high-level, compliance-focused national benchmark aligned with ISO/IEC 27001, the NIST SP 800 series provides the specific, actionable technical implementation guidelines needed to resolve the concrete security gaps identified during the evaluation.

References

[1] I. Afrianto, T. Suryana dan S. Atin, “Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI-SNI ISO/IEC 27001:2009 Studi Kasus Perguruan Tinggi X,” ULTIMA InfoSys, vol. VI, no. 1, 2015. doi: https://doi.org/10.31937/si.v6i1.278

[2] L. D. A. Jelita, M. N. A. Azam dan A. Nugroho, “Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/IEC 27001:2022,” Jurnal SAINTEKOM, vol. 14, no. 1, pp. 84-94, 2024. doi: https://doi.org/10.33020/saintekom.v14i1.623

[3] D. Zalukhu, V. Yasin dan A. B. Yulianto, “EVALUASI KEAMANAN SISTEM INFORMASI AKADEMIK DI STMIK JAYAKARTA BERDASARKAN ISO/IEC 27001:2022,” Indonesian Journal on Information System, vol. 10, no. 2, 2025. doi: https://doi.org/10.36549/ijis.v10i2.412

[4] F. A. S. Ningrum, Y. Riwanto, I. Y. R. Pratiwi dan M. A. Fikri, “ANALISIS KEAMANAN SISTEM INFORMASI PERGURUAN TINGGI BERBASIS INDEKS KAMI,” JIP (Jurnal Informatika Polinema), vol. 10, no. 3, 2024. doi: https://doi.org/10.33795/jip.v10i3.5154

[5] R. Sinaga, “Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022,” Jurnal Teknik Informatika dan Sistem Informasi, vol. 9, no. 3, 2023. doi: https://doi.org/10.28932/jutisi.v9i3.6850

[6] R. R. Wijayanti, “IMPLEMENTASI OCTAVE-S DAN STANDAR PENGENDALIAN ISO 27001:2013 PADA MANAJEMEN RISIKO SISTEM INFORMASI PERGURUAN TINGGI” JURNAL PETIR, vol. 11, no. 2, 2018. doi: https://doi.org/10.33322/petir.v11i2.351

[7] M. Y. Putra dan D. Tjahjadi, "Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001," Jurnal Penelitian Ilmu Komputer, System Embedded & Logic, vol. 6, no. 1, pp. 95-104, 2018. doi: https://doi.org/10.33558/piksel.v6i1.1404

[8] G. Fitria, D. Yuniarto dan D. Setiadi, "Evaluasi Keamanan Sistem Pajak Daerah Online Kabupaten Sumedang Menggunakan Indeks Keamanan Informasi 5.0," Jurnal Teknik Mesin, Industri, Elektro dan Informatika, vol. 4, no. 1, pp. 232-242, 2025. doi: https://doi.org/10.55606/jtmei.v4i1.4817

[9] S. Paramita, S. A. Siregar, R. A. Damanik dan M. D. Irawan, "Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013," Bulletin of Information Technology (BIT), vol. 3, no. 4, pp. 374 - 379, 2022. doi: https://doi.org/10.47065/bit.v3i4.421

[10] F. A. Basyarahil,, H. M. Astuti dan B. C. Hidayanto, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya," JURNAL TEKNIK ITS, vol. 6, no. 1, pp. 2301-9271, 2017.

[11] M. A. Gumelar, H. W. Nugroho dan M. S. Hasibuan, "IMPLEMENTASI INDEKS KAMI DI UNIVERSITAS XYZ," Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), vol. 12, no. 6, pp. 1463-1474, 2025. doi: https://doi.org/10.25126/jtiik.2025126

[12] J. Alberto dan C. M. Karyati, "Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan ISO 27001:2022 (Studi Kasus Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan)," Jurnal Ilmiah KOMPUTASI, vol. 22, no. 4, 2023.

[13] M. Izzani, N. Nellatul, A. Ismatul dan A. Hamdani, "Evaluation of the Implementation of Information Security at SIAKAD Ibrahimy University Based on ISO/IEC 27001:2022," JURNAL ILMIAH SISTEM INFORMASI (JUSI), vol. 5, no. 1, pp. pp. 175 - 185, 2026. doi: https://doi.org/10.51903/d3bktm29

[14] A. R. Riswaya, A. Sasongko dan A. Maulana, "EVALUASI TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI MENGGUNAKAN INDEKS KAMI UNTUK PERSIAPAN STANDAR SNI ISO/IEC 27001 (STUDI KASUS: STMIK MARDIRA INDONESIA)," Jurnal Computech & Bisnis, vol. 14, no. 1, pp. 10-18, 2020.

[15] A. I. Mafiana, L. Hanun, H. M. Ilmi dan S. Febriliani, "IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO 27001 PADA SISTEM INFORMASI AKADEMIK," JDBIM (Journal of Digital Business and Innovation Management), vol. 2, no. 2, pp. 139-163, 2023. doi: 10.1234/jdbim.v2i2.57580

[16] N. D. Ramadhani, W. H. N. Putra dan A. D. Herlambang, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 4, no. 5, pp. hlm. 1490-1498, 2020. http://j-ptiik.ub.ac.id

[17] M. Yunella, A. D. Herlambang dan W. H. N. Putra, "Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 3, no. 10, pp. hlm. 9552-9559, 2019. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6521

[18] M. Rizkillah, "EVALUASI KEAMANAN INFORMASI PERGURUAN TINGGI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) VERSI 5.0," Jurnal Cakrawala Ilmiah, vol. 3, no. 10, 2024.

[19] A. Amaliyah, "Evaluasi Mandiri Pada Sistem Penyelenggaraan Elektronik Berdasarkan Indeks Keamana Informasi (KAMI) Dan ISO 27001 (Studi Kasus: Sistem Litera Uninus)," Jurnal Sistem Informasi, J-SIKA, vol. 05, no. 02, 2023. https://ejournal.unibba.ac.id/index.php/j-sika/article/view/1301

[20] A. S. Adung, "Evaluasi Indeks Keamanan Informasi (KAMI) Pada Pengamanan Penyelenggaraan Sistem Elektronik Berdasarkan ISO 27001 (Studi Kasus: STT Pratama Adi)," Jurnal Sistem Informasi, J-SIKA, vol. 05, no. 01, p. 2716 – 4195, 2023.

[21] Badan Siber dan Sandi Negara (BSSN), Indeks Keamanan Informasi (KAMI) Versi 5.0: Panduan Evaluasi Keamanan Informasi. Jakarta: BSSN, 2023. [Online]. https://www.bssn.go.id/indeks-kami

[22] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Jakarta: Sekretariat Negara, 2022.

[23] Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Jakarta: Sekretariat Negara, 2019.