Computer Engineering and Applications Vol. 15, No. 2, June 2026

An Information Security Maturity Evaluation of the BKO District Court Based on the KAMI Index Version 5.0

Muhammad Tulus Akbar[1], Rayasa Gussati[2], M. Aditya R. Pradiva[3], Refina[4], Elsa Youri Ferlica[5], Thedy Mulya Afriandi[6], Dina Ayu Indah Lestari[7], Hasim Husadi[8]

Department of Information System Faculty of Science and Technology, University Merangin,Indonesia
**muhammadtuluseducation@gmail.com*

ABSTRACT

Information security is a vital component in institutional IT operations, especially for Electronic System Operators (ESO). Effective governance is essential to ensure data protection, integrity, and availability. The readiness evaluation of the BKO District Court, conducted using the KAMI Index version 5.0 based on ISO/IEC 27001:2022, assessed seven areas: information security governance, risk management, information security framework, asset and technology management, personal data protection, and supplementary controls involving third parties. The assessment applied five implementation levels and maturity levels I–V. The Court scored 14 in the electronic system category (low dependency) and achieved an overall score of 913 with a "Good" rating. The highest maturity levels were recorded in risk management and the information security framework (Level V), while other areas ranged from Levels III to IV. Overall, the results show that the BKO District Court has a well-developed and consistently implemented information security governance structure, though enhancements in asset management and personal data protection are still required to achieve optimal maturity under SNI ISO/IEC 27001:2022.

Keywords: KAMI Index, ISO/IEC 27001:2022, Information Security, Electronic System Operator (ESO), Information and Communication Technology (ICT).

1. INTRODUCTION

Protection in information security is essential for ensuring operational continuity in organizations that rely on digital systems, as vulnerabilities may lead to data breaches and service disruptions [1]. Therefore, comprehensive safeguards are required to secure data and all supporting components—systems, networks, and hardware involved in information processing, storage, and distribution [2]. The rapid development of technology further increases the complexity of maintaining security, evidenced by the rise of sophisticated cyber attacks such as phishing, malware, ransomware, and vulnerability exploitation, all of which can cause significant losses [3], [4]. These threats demand serious attention, particularly for small enterprises that often lack strong security controls and are highly vulnerable to cybercrime [5].

Digital transformation undertaken without proper planning or adequate controls further heightens exposure to cyber risks [6]. Thus, organizations need a strong understanding of preventive and mitigative measures, supported by increased awareness among data managers through continuous training and strict security policies to maintain privacy and confidentiality [7], [8]. One effective approach is

implementing an Information Security Management System (ISMS), especially for institutions providing public information services or operating in strategic sectors [2]. An ISMS optimizes resource use, guides threat mitigation, and helps reduce incidents that may result in substantial losses [5], [9].

This study evaluates the readiness and governance of information security at the BKO District Court as an Electronic System Operator (ESO) using the Indeks Keamanan Informasi (KAMI) version 5.0, which emphasizes maturity and readiness based on ISO/IEC 27001:2022. In line with current developments, the assessment refers to the 2022 information security governance guidelines, with the KAMI Index serving as the primary evaluation tool [2]. The results are intended to measure the institution's readiness, completeness, and maturity and to guide the ESO in enhancing information security to meet the SNI ISO/IEC 27001:2022 standard [1].

2. METHOD

The study employed a descriptive–evaluative method to assess the readiness, governance, and maturity of information security implementation within the Electronic System Operator (ESO) [4]. This approach provides a comprehensive overview of the actual information security conditions based on the KAMI evaluation aligned with the ISO/IEC 27001:2022 standard [10]. The complete research stages are shown in Figure 1.

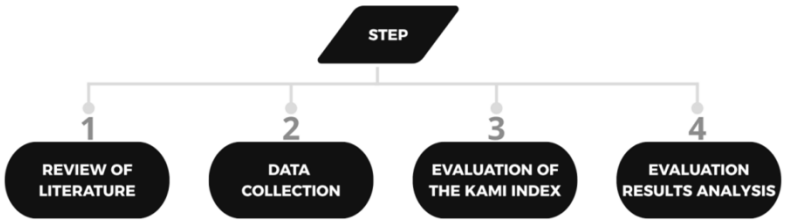

FIGURE 1. Research Stages Evaluation KAMI Index.

2.1 REVIEW OF LITERATURE

The literature review strengthens the understanding of essential concepts, principles, and frameworks in information security evaluation [2]. The primary reference is the KAMI Index issued by BSSN, which functions as an instrument for assessing readiness, governance, and maturity in Indonesia [11], complemented by the ISO/IEC 27001:2022 standard as the global benchmark for ISMS implementation [4], [12]. This review also provides a conceptual foundation for key information security aspects—governance, risk management, security frameworks, asset management, and technology protection [3], [9]—and examines prior studies using the KAMI Index to identify research gaps and reinforce the theoretical basis for the analytical model applied in this study [2], [3], [13], [14].

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

2.2 DATA COLLECTION

Data collection was conducted to obtain up-to-date information on the organization's information security implementation [2]. The methods used included interviews, observations, and document analysis relevant to the KAMI Index assessment [15]. Interviews with IT administrators provided insight into policy implementation [9], observations examined infrastructure and security practices, and document reviews analyzed internal policies, guidelines, and reports [16]. The collected data were then organized into the five main KAMI Index areas to evaluate readiness and maturity in information security management [1], [17].

The evaluation used the KAMI Index version 5.0 developed by BSSN, which measures the readiness and maturity of Electronic System Operators (ESO) in alignment with ISO/IEC 27001:2022 [18]. The instrument assesses five key areas—governance, risk management, security framework, asset management, and security technology—along with two supplementary components: Personal Data Protection (PDP) and the Supplement for third-party and cloud service security [2]. Each area follows three maturity stages: establishing a basic framework, ensuring consistent controls, and enabling continuous improvement [1]. The resulting scores reflect the organization's overall readiness level [2], [19] and were used to identify priority areas for strengthening information security at the BKO District Court, as shown in Table 1.

TABLE 1.
Readiness Level Scores by Security Category.

	Security Level Category		
Information Security Status	1	2	3
Not Implemented	0	0	0
In the Planning Phase	1	2	3
Partially Implemented	2	4	6
Fully Implemented	3	6	9
Not Applicable	0	0	0

Table 1 shows the security category scores based on the status of information security implementation [2]. The implementation status is classified into four levels—Not Implemented, In the Planning Stage, Partially Implemented, and Fully Implemented—with score weights of 0, 1–3, 2–6, and 3–9. The Not Applicable/Not Relevant status is scored 0 when it does not match the organizational context. The assessment follows COBIT and CMMI maturity levels (I–V) with intermediate levels (I+–IV+) to reflect gradual progress. According to SNI ISO/IEC 27001:2022, the minimum expected readiness level is III+, indicating consistent, documented, and systematic implementation of information security [2], [20].

3. RESULT

This chapter presents the research findings obtained through the application of the KAMI Index version 5.0 as the evaluation instrument, in order to assess the level of information security management readiness at the BKO District Court.

3.1 ELECTRONIC SYSTEM CATEGORY

The electronic system category evaluates the classification level of an organization's electronic systems [9]. It includes three dependency levels—low, high, and strategic—assessed using ten indicator questions that describe institutional characteristics. The assessment produced a total score of 14, placing the system in the low-dependency category. The three categories are shown in Table 2.

TABLE 2.
Electronic System Classification Score.

Level of ICT Dependency	Lower Limit	Upper Limit	Classification
A	10	15	Low
B	16	34	High
C	35	50	Strategic

The BKO District Court's electronic system scored 14, placing it in the low category, indicating limited ICT dependency confined to administrative and operational tasks. Thus, system disruptions would not significantly affect core functions. These results serve as an initial basis for strengthening policies and basic information security controls to enhance ICT readiness and reliability [12].

3.2 INFORMATION SECURITY GOVERNANCE

The information security governance section assesses an organization's readiness in carrying out its roles and responsibilities for managing information security [14]. The evaluation uses four implementation standards—not implemented, planning, partially implemented, and fully implemented—and consists of 22 indicator questions. These indicators include 8 items in Security Category I (Maturity Level II), 5 items in Category II (Maturity Level II), 3 items in Category II (Maturity Level III), and 6 items in Category III (Maturity Level IV). Detailed results are shown in Table 3.

TABLE 3.
Information Security Governance Evaluation Score.

Security Category	Number of Questions	Score
1	8	24
2	8	48
3	6	54
Total	**22**	**126**

Based on the field findings, the Information Security Governance section scored 126 from 22 questions across three categories: 24 for Category I, 48 for Category II, and 54 for Category III. These results show that the BKO District Court has reached Maturity Levels I, II, and III, surpassing the minimum Level III+ requirement under SNI ISO/IEC 27001:2022. Although implementation is consistent, further

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

improvements are needed to achieve higher maturity levels, particularly in governance strengthening and risk management enhancement [9].

3.3 INFORMATION SECURITY RISK MANAGEMENT

The information security risk management section evaluates the organization's readiness in implementing risk management as the basis for developing security strategies [11]. The assessment uses four implementation categories— not implemented, planning, partially implemented, and fully implemented—across 16 indicator questions. These include 10 items in Security Category I (Maturity Level II), 2 in Category II (Maturity Level III), 2 in Category II (Maturity Level IV), and 2 in Category III (Maturity Level V). Detailed results are presented in Table 4.

TABLE 4.
Information Security Risk Management Evaluation Score.

Security Category	Number of Questions	Score
1	10	30
2	4	24
3	2	18
Total	**16**	**72**

Based on the recapitulation, the information security risk management section scored 72 from 16 questions across three categories: 30 for Category 1, 24 for Category 2, and 18 for Category 3. These results indicate a moderate maturity level, with most controls implemented but still requiring better consistency and effectiveness to meet the optimal SNI ISO/IEC 27001:2022 standard [17].

3.4 INFORMATION SECURITY MANAGEMENT FRAMEWORK

The information security management framework evaluates the organization's readiness in developing and implementing information security policies, procedures, and strategies [2]. The assessment uses four implementation categories— not implemented, planning, partially implemented, and fully implemented—across two subcategories: (1) policy and procedure management (22 indicators, Maturity Levels II–IV) and (2) strategy and program management (10 indicators, Maturity Levels II–V). Overall, the results indicate a mature and well-structured framework, as shown in Table 5.

TABLE 5.
Evaluation Score for the Information Security Management Framework.

Security Category	Number of Questions	Score
1	12	36
2	11	66
3	10	90
Total	**33**	**192**

The information security management framework achieved a total score of 192 from 33 questions across three categories: 36 for Category I, 66 for Category II, and 90 for Category III. These results show that the BKO District Court has reached Maturity Level III (Defined and Consistent) and is progressing toward Level IV (Managed and Measurable) [19]. Although the framework is effectively and consistently implemented, improvements in performance measurement and continuous management are still required to achieve optimal maturity under SNI ISO/IEC 27001:2022 [12].

3.5 INFORMATION ASSET MANAGEMENT

The information asset management aspect assesses the effectiveness of protecting hardware, software, data, and networks across their lifecycle, using four implementation levels: not implemented, planning, partially implemented, and fully implemented [11]. It consists of three subcategories—information asset management (30 indicators, Levels II–III), cloud service security (11 indicators, Level III), and physical security (12 indicators, Levels II–III). Overall, the system is well-structured and effective, though monitoring and cloud service governance still require improvement to fully meet SNI ISO/IEC 27001:2022, as shown in Table 6.

TABLE 6.
Evaluation Score for Information Asset Management.

Security Category	Number of Questions	Score
1	27	81
2	19	114
3	7	63
Total	**53**	**258**

The information asset management section scored 258 from 53 questions (81 for Category I, 114 for Category II, and 63 for Category III), indicating that the BKO District Court has reached Maturity Level III and is progressing toward Level IV. Asset management is implemented systematically—covering inventory, protection, cloud services, and physical security [2], though improvements in control effectiveness and periodic evaluation are still needed to meet SNI ISO/IEC 27001:2022 [21].

3.6 INFORMATION SECURITY TECHNOLOGY

The information security technology aspect assesses the effectiveness, consistency, and completeness of technologies used to protect organizational information assets [19]. Using five implementation categories, it consists of one subcategory with 35 indicators (Maturity Levels I–IV), covering access control, network monitoring, data protection, and incident detection. Overall, the results show strong and sustainable technology implementation, as detailed in Table 7.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

TABLE 7.
Evaluation Score for Information Security Technology.

Security Category	Number of Questions	Score
1	14	41
2	15	86
3	6	54
Total	**35**	**181**

The information security technology aspect scored 181 from 35 indicators across three categories: 41 for Category I, 86 for Category II, and 54 for Category III. These results show that the BKO District Court has reached Maturity Level III+ and is progressing toward Level IV, reflecting effective implementation of access control, network monitoring, and data/system protection [21]. Improvements in system integration and incident detection are still required to achieve optimal maturity under SNI ISO/IEC 27001:2022 [5].

3.7 PERSONAL DATA PROTECTION

The PDP category evaluates the comprehensiveness, consistency, and effectiveness of personal data security controls [8]. Using four implementation categories, it consists of 16 indicators: 4 in Security Category I (Level II), 2 in Category II (Level II), and 10 in Category II (Level III). Overall, PDP implementation is fairly good, though consistency of controls and adherence to data security policies still require improvement, as shown in Table 8.

TABLE 8.
Evaluation Score for Personal Data Protection.

Security Category	Number of Questions	Score
1	4	12
2	12	72
3	0	0
Total	**16**	**84**

Based on the evaluation, the PDP category scored 84 from 16 questions: 12 for Category I, 12 for Category II, and 60 for Category III. These results show that the BKO District Court has reached Maturity Level III (Defined and Consistent) in personal data protection [22], with policies and mechanisms applied systematically [23]. However, improvements in monitoring, compliance auditing, and employee awareness are still needed to reach higher maturity in accordance with SNI ISO/IEC 27001:2022 on Personal Data Protection [24].

3.8 SUPPLEMENT

The supplement section serves as the final evaluation component, assessing the effectiveness of technology use and third-party involvement in protecting information assets [25]. Using four implementation levels, it focuses on third-party security, including risk management, security policies, service continuity, and the management

of subcontractors, assets, and incidents. Overall, this section shows the extent to which the BKO District Court has applied integrated security policies and controls in its third-party collaborations. Detailed results are provided in Table 9.

TABLE 9.
Supplement Evaluation Score.

Category	Total Questions	Score
1	27	3,00
Total	**27**	**100%**

Based on the evaluation, the supplement section scored an average of 3.00 from 27 questions, achieving 100%. This indicates that the BKO District Court has implemented highly effective third-party security controls, including risk management, security policies, asset control, incident handling, and service continuity, with consistent and well-documented oversight [14]. Overall, this section has reached a high maturity level in line with SNI ISO/IEC 27001:2022, supporting continuous improvement of information security governance at the BKO District Court [26].

3.9 DASHBOARD

The KAMI Index version 5.0 evaluation shows that the BKO District Court has achieved maturity across all areas—governance, risk management, framework, assets, technology, personal data protection, and third-party security. These results indicate readiness aligned with SNI ISO/IEC 27001:2022 and provide a basis for strengthening future information security strategies [11]. Figure 2 presents the maturity levels for each area.

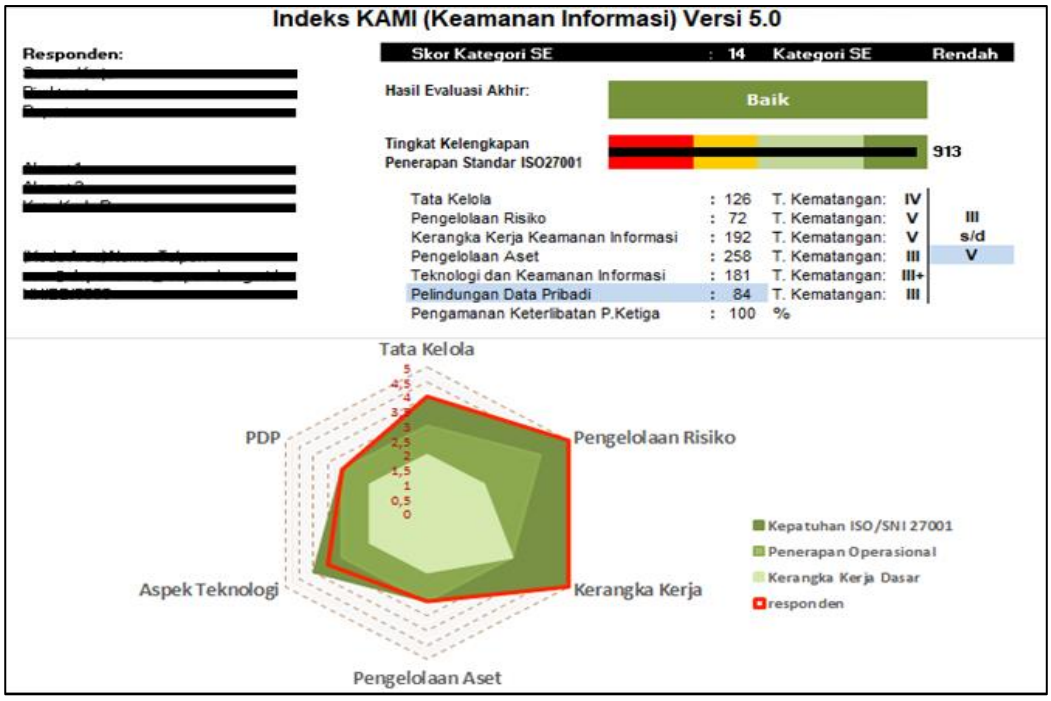

FIGURE 2. KAMI Index 5 Evaluation Dashboard

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

The final evaluation shows that the BKO District Court scored 14 in the Electronic System (SE) category—classified as low—and 913 overall with a "Good" rating, indicating ISO/IEC 27001 compliance. Figure 2 highlights key focus areas, including ISO/SNI 27001 compliance, governance, risk management, framework, assets, technology, and PDP. The strongest results are in risk management and the information security framework, both at Maturity Level V (Optimal). Overall, the Court has implemented a stable, measurable, and internationally aligned information security system [12].

4. CONCLUSION

Based on the analysis and evaluation presented in the previous chapter, the following conclusions were drawn:

1. The evaluation results show that the BKO District Court scored 14 in the Sistem Elektronik (SE) Category—classified as low—and achieved a total score of 913 with a "Good" rating, indicating strong ISO/IEC 27001 implementation aligned with the SE classification.
2. The assessment results show that the BKO District Court achieved the following scores: Information Security Governance (126, Level IV), Risk Management (72, Level V), Information Security Framework (192, Level V), Asset Management (258, Level III), Information Security Technology (181, Level III+), Personal Data Protection (84, Level III), and Third-Party Security (100%).
3. The KAMI Index version 5.0 evaluation shows that the BKO District Court has achieved a strong level of readiness and maturity in implementing its information security framework [12]. These results provide a basis for ICT administrators to further enhance information security, especially in areas not yet optimal, to ensure alignment with the SNI ISO/IEC 27001:2022 standard [2].

REFERENCES

[1] T. N. Khusna And B. Sugiantoro, "Pengukuran Tingkat Keamanan Informasi Pada Upt-Psi Universitas Muria Kudus Berdasarkan Indeks Keamanan Informasi (Kami) Versi 4.2," *Jipi (Jurnal Ilm. Penelit. Dan Pembelajaran Inform.*, Vol. 8, No. 3, Pp. 847–856, 2023, Doi: 10.29100/Jipi.V8i3.3720.

[2] H. Imtikhan Azmi, Tulus_Akbar, B. Tasya Kumala Dewi, And B. Sugiantoro, "Evaluasi Tingkat Kesiapan Keamanan Informasi Pada Smk Xyz Menggunakan Indeks Kami Versi 4.2," *Cyber Secur. Dan Forensik Digit.*, Vol. 7, No. 1, Pp. 42–49, 2024, Doi: 10.14421/Csecurity.2024.7.1.4422.

[3] Fauzia Anis Sekar Ningrum, Yudha Riwanto, Inggrid Yanuar Risca Pratiwi, And Muhammad Ainul Fikri, "Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks Kami," *J. Inform. Polinema*, Vol. 10, No. 3, Pp. 437–444, 2024, Doi: 10.33795/Jip.V10i3.5154.

[4] W. A. Karunia, A. F. Zahra, And Y. Amrozi, "Kajian Ancaman Baru Dalam Keamanan Informasi : Systematic Literature Review Pada Kerentanan Cyber

Security Pasca-Pandemi Evaluating Emerging Threats In Information Security : A Systematic Literature Review On Post-Pandemic Cybersecurity Vulnerabilities," *Cybersecurity Dan Forensik Digit.*, Vol. 8, No. 1, Pp. 10–16, 2025.

[5] M. N. Y. Marican, S. A. Razak, A. Selamat, And S. H. Othman, "Cyber Security Maturity Assessment Framework For Technology Startups: A Systematic Literature Review," *Ieee Access*, Vol. 11, No. January, Pp. 5442–5452, 2023, Doi: 10.1109/Access.2022.3229766.

[6] D. I. Khamil, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan Iso/Iec 27001:2013 (Studi Kasus : Diskominfo Kabupaten Gianyar)," *Jatisi (Jurnal Tek. Inform. Dan Sist. Informasi)*, Vol. 9, No. 3, Pp. 1948–1960, 2022, Doi: 10.35957/Jatisi.V9i3.2310.

[7] A. Bakhtiar And F. Salsabila Hidayat, "Evaluasi Sistem Manajemen Keamanan Informasi Berdasarkan Penilaian Indeks Kami V.4.2 Pada Dinas Xyz Provinsi Jawa Tengah," *Ind. Eng. Online J.*, Vol. 12, No. 4, 2023, [Online]. Available: Https://Ejournal3.Undip.Ac.Id/Index.Php/Ieoj/Article/View/41401

[8] N. Sun *Et Al.*, "Defining Security Requirements With The Common Criteria: Applications, Adoptions, And Challenges," *Ieee Access*, Vol. 10, Pp. 44756–44777, 2022, Doi: 10.1109/Access.2022.3168716.

[9] S. Clarissa And G. Wang, "Assessing Information Security Management Using Iso 27001:2013," *J. Indones. Sos. Teknol.*, Vol. 4, No. 9, Pp. 1361–1371, 2023, Doi: 10.59141/Jist.V4i9.739.

[10] S. Gaba *Et Al.*, "A Systematic Analysis Of Enhancing Cyber Security Using Deep Learning For Cyber Physical Systems," *Ieee Access*, Vol. 12, No. December 2023, Pp. 6017–6035, 2023, Doi: 10.1109/Access.2023.3349022.

[11] R. Savitri, Firmansyah, Dworo, And M. S. Hasibuan, "Information Security Measurement Using Index Kami At Metro City," *J. Appl. Data Sci.*, Vol. 5, No. 1, Pp. 33–45, 2024, Doi: 10.47738/Jads.V5i1.152.

[12] T. T. Wulansari And D. Novandi, "Evaluation Of Information Security Management Using The Kami Index Framework," *2022 Int. Conf. Sci. Inf. Technol. Smart Adm. Icsintesa 2022*, No. 4, Pp. 173–177, 2022, Doi: 10.1109/Icsintesa56431.2022.10041714.

[13] R. Dewantara And B. Sugiantoro, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Jaringan (Studi Kasus: Uin Sunan Kalijaga Yogyakarta)," *J. Teknol. Inf. Dan Ilmu Komput.*, Vol. 8, No. 6, P. 1137, 2021, Doi: 10.25126/Jtiik.2021863123.

[14] S. Paramita, S. A. Siregar, R. A. Damanik, And ..., "Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (Kami) Iso 27001: 2013," *Bull. Inf. ...*, Vol. 3, No. 4, Pp. 374–379, 2022, [Online]. Available: Https://Journal.Fkpt.Org/Index.Php/Bit/Article/View/421%0ahttps://Journal.Fkpt.Org/Index.Php/Bit/Article/Download/421/263

[15] M. T. Akbar And M. U. Siregar, "A Survey On Software Requirements Engineering In Information Technology Institutions," Vol. 9, No. 2, Pp. 253–264, 2024.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

[16] N. D. Ramadhani, W. H. N. Putra, And A. D. Herlambang, "Evaluasi Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kabupaten Malang Menggunakan Indeks Kami (Keamanan Informasi)," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, Vol. 4, No. 5, Pp. 1490–1498, 2020, [Online]. Available: Https://J-Ptiik.Ub.Ac.Id/Index.Php/J-Ptiik/Article/View/7259

[17] R. Habibullah, M. T. Nuruzzaman, And A. Mulyanto, "Evaluasi Keamanan Sistem Informasi Dengan Indeks Kami Dan Cobit 5 Di Pesantren," *Cyber Secur. Dan Forensik Digit.*, Vol. 7, No. 2, Pp. 69–80, 2024, Doi: 10.14421/Csecurity.2024.7.2.4576.

[18] Online, "Konsultasi Dan Assesment Indeks Kami." Accessed: Mar. 13, 2025. [Online]. Available: Https://Www.Bssn.Go.Id/Indeks-Kami/

[19] F. Wijayanti, D. I. Sensuse, A. A. Putera, And A. Syahrizal, "Assessment Of Information Security Management System: A Case Study Of Data Recovery Center In Ministry Xyz," *2020 3rd Int. Conf. Comput. Informatics Eng. Ic2ie 2020*, Pp. 393–398, 2020, Doi: 10.1109/Ic2ie50715.2020.9274574.

[20] M. . H. R.Y Rahman, "Evaluasi Keamanan Informasi Pada Sman 1 Tanggamus Menggunakan Indeks Kami Versi 4.2," *J. Fasilkom*, Vol. 13, No. 2, Pp. 181–187, 2023.

[21] H. Zhang, Y. Pan, Z. Lu, J. Wang, And Z. Liu, "A Cyber Security Evaluation Framework For In-Vehicle Electrical Control Units," *Ieee Access*, Vol. 9, Pp. 149690–149706, 2021, Doi: 10.1109/Access.2021.3124565.

[22] C. C. Chan, C. Z. Yang, And C. F. Fan, "Security Verification For Cyber-Physical Systems Using Model Checking," *Ieee Access*, Vol. 9, Pp. 75169–75186, 2021, Doi: 10.1109/Access.2021.3081587.

[23] M. Irfan, M. Hassan, N. Hassan, M. Habib, S. Khan, And A. M. Nasruddin, "Project Management Maturity And Organizational Reputation: A Case Study Of Public Sector Organizations," *Ieee Access*, Vol. 8, Pp. 73828–73842, 2020, Doi: 10.1109/Access.2020.2988511.

[24] B. Alkhazi, M. Alshaikh, S. Alkhezi, And H. Labbaci, "Assessment Of The Impact Of Information Security Awareness Training Methods On Knowledge, Attitude, And Behavior," *Ieee Access*, Vol. 10, No. November, Pp. 132132–132143, 2022, Doi: 10.1109/Access.2022.3230286.

[25] 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.

[26] Y. Kawanishi, H. Nishihara, H. Yoshida, H. Yamamoto, And H. Inoue, "A Study On Threat Analysis And Risk Assessment Based On The 'Asset Container' Method And Cwss," *Ieee Access*, Vol. 11, No. January, Pp. 18148–18156, 2023, Doi: 10.1109/Access.2023.3246497.