CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 9, No. 1, Mei 2026, hlm. 88-97

Evaluasi Kesiapan Keamanan Informasi BAWASLU ABC Menggunakan Indeks KAMI 5.0

Muhammad Tulus Akbar[1], Ratu Tasya Veronica[2], Rismaya Ika Widyana[3], Habib Nurahman[4]

Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Merangin, Jambi[1,2,3,4]
Email: [1]muhammadtuluseducation@gmail.com

Abstrak

Keamanan informasi merupakan elemen vital yang berperan dalam Penyelenggara Sistem Elektronik (PSE). Indeks KAMI 5.0 tidak hanya sebagai pembaharuan dari versi yang tersedia sebelumnya tetapi mengedepankan terkait ancaman siber terkini, transformasi digital dan privasi pihak ketiga, selaras dengan regulasi peraturan perlindungan data pribadi. Evaluasi tingkat keamanan BAWASLU ABC mengacu kepada SNI ISO/IEC 27001:2022. Penilaian dilakukan pada tujuh kategori yaitu tata kelola keamanan informasi, pengelolaan risiko, kerangka kerja keamanan informasi, pengelolaan aset dan teknologi informasi, perlindungan data pribadi, serta suplemen terkait keterlibatan pihak ketiga. Metode yang digunakan adalah deskriptif evaluatif dengan cara pengumpulan data melalui tahap wawancara dan observasi berkas. Hasil temuan lapangan menunjukan kategori sistem elektronik menunjukan skor sebesar 14 dan masuk dalam kategori baik, pengelolaan risiko dengan skor 72 dan kerangka kerja keamanan informasi dengan skor 192 masuk dalam tingkat keamanan V yang berarti (Terkelola dan Terukur). Sedangkan empat kategori lainnya berada pada tingkat keamanan III dan IV. Hasil ini menunjukan bahwa BAWASLU ABC telah mengadopsi struktur tata kelola keamanan informasi yang telah berkembang dengan baik dan konsisten, namun masih diperlukan peningkatan pada aspek pengelolaan aset informasi dan perlindungan data pribadi agar mencapai tingkat kematangan optimal sesuai standar SNI ISO/IEC 27001:2022.

Kata kunci: Indeks KAMI, ISO/IEC 27001:2022, Penyelenggara Sistem Elektronik (PSE), Teknologi Informasi Komunikasi (TIK)

Abstract

Information Security Readiness Evaluation of BAWASLU ABC Using KAMI Index 5.0

Information security is a vital element in the implementation of Electronic System Providers (ESP). The KAMI Index version 5.0 is not merely an update of the previous version, but also addresses current cyber threats, digital transformation, and third-party privacy in alignment with personal data protection regulations. This study evaluates the level of information security at BAWASLU ABC with reference to the SNI ISO/IEC 27001:2022 standard. The assessment was conducted across seven categories, namely information security governance, risk management, information security framework, asset and information technology management, personal data protection, and supplementary aspects related to third-party involvement. A descriptive qualitative method was employed, with data collected through interviews and document observation. The findings indicate that the electronic system category achieved a score of 14 and was classified as good, while the risk management domain scored 72 and the information security framework scored 192, both reaching security maturity Level V (Managed and Measurable). The remaining four categories were at maturity Levels III and IV. Overall, the results demonstrate that BAWASLU ABC has adopted a well-developed and consistently implemented information security governance structure; however, improvements are still required in the areas of information asset management and personal data protection to achieve optimal maturity in accordance with the SNI ISO/IEC 27001:2022 standard.

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

1. PENDAHULUAN

Perlindungan bidang keamanan informasi merupakan komponen krusial pada aspek keberlangsungan operasional organisasi yang mengandalkan sistem digital, karena kelemahan dalam aspek ini dapat menimbulkan risiko kebocoran data dan gangguan layanan (Khusna and Sugiantoro, 2023). Oleh karena itu, diperlukan perlindungan terhadap data dan seluruh komponen pendukungnya, termasuk sistem, jaringan, serta perangkat keras yang berperan dalam proses

pengolahan, penyimpanan, dan distribusi informasi (Imtikhan Azmi et al., 2024).

Kemajuan teknologi yang cepat menyebabkan meningkatnya kompleksitas dalam menjaga keamanan informasi, yang terlihat dari maraknya serangan siber dengan tingkat kecanggihan serta dampak kerugian yang semakin besar (Fauzia Anis Sekar Ningrum et al., 2024). Ancaman seperti phishing, malware, ransomware, dan eksploitasi celah keamanan perangkat lunak masih menjadi persoalan yang belum sepenuhnya dapat diantisipasi oleh berbagai organisasi, baik berskala kecil maupun besar (Karunia, Zahra and Amrozi, 2025). Dalam konteks risiko bisnis, permasalahan ini seharusnya mendapatkan perhatian serius dari para pembuat kebijakan, kejahatan *cyber* kerap menargetkan pelaku usaha kecil yang memiliki sistem keamanan relatif lemah dan rentan terhadap serangan (Marican et al., 2023). Tercatat pada tahun 2019 tercatat sebanyak 148 kasus *cybercrime* yang menargetkan lembaga penyelenggara pemilu di seluruh Indonesia (Nyoman Amie Sandrawati, 2024). Oleh sebab itu diperlukan peningkatan keamanan data dan kesalahan manusia dalam menyelengarakan informasi elektronik agar dapat melingdungi hak demokrasi (Green, Sarrafzadeh and Anwar, 2025).

Salah satu langkah yang dapat dilakukan untuk menghindari ancaman kejahatan siber adalah dengan menerapkan SMKI (Sistem Manajemen Keamanan Informasi), terutama bagi kelembagaan atau penyedia sarana layanan informasi data publik yang memiliki tingkat kepentingan tinggi dan bersifat strategis (Imtikhan Azmi et al., 2024). Penerapan SMKI juga berfungsi untuk mengoptimalkan pemanfaatan sumber daya yang tersedia serta menjadi panduan dalam pengendalian dan mitigasi berbagai ancaman keamanan informasi (Clarissa and Wang, 2023). Selain itu, agar dapat meminimalisir terjadinya ancaman yang berakibatkan kerugian yang masif (Marican et al., 2023).

Standar keamanan informasi di Indonesia diukur melalui Indeks Keamanan Informasi (KAMI), yang berperan selaku instrumen untuk meninjau serta mengkaji tingkat kesiapan, kelengkapan, serta kematangan penerapan tata kelola keamanan informasi sesuai karakteristik yang diacu dalam SNI ISO/IEC 27001 (Imtikhan Azmi et al., 2024). Evaluasi Indeks KAMI dirancang untuk diterapkan oleh berbagai organisasi Penyelengara Sistem Elektronik (PSE), baik pemerintah maupun non-pemerintah, guna mengukur tingkat kematangan manajemen keamanan layanan informasi digital (Dewantara and Sugiantoro, 2021).

Penelitian dengan model evaluasi menggunakan Indeks KAMI telah banyak dilakukan sebelumnya untuk mengevaluasi kesiapan keamanan informasi pada berbagai intansi pemerintah dan organisasi publik. Banyak studi masih mengacu kepada Indeks KAMI versi 4.2 yang berbasis ISO/IEC 27001:2013 dan telah diterapkan secara luas oleh organiasi PSE, sehingga menyediakan referensi dan pola evaluasi yang mapan (Imtikhan Azmi et al., 2024). Namun, seiring dengan meningkatnya kompleksitas ancaman siber dan kebutuhan perlindungan data pribadi, penelitian terbaru cenderung menggunakan Indeks KAMI versi 5.0 yang telah disesuaikan dengan ISO/IEC 27001:2022 dan menekankan penilaian berbasis tingkat kematangan, keterlibatan pihak ketiga, serta aspek privasi data (Fauzia Anis Sekar Ningrum et al., 2024).

Penelitian ini bertujuan untuk mengukur tingkat kesiapan keamanan informasi serta penerapan tata kelola keamanan pada organisasi PSE (Penyelenggara Sistem Elektronik), yaitu BAWASLU (Badan Pengawas Pemilu) ABC di tingkat kabupaten. Nama organisasi disamarkan agar menjaga kerahasiaan keamanan informasi lembaga dan menjaga kerahasiaan data yang terdapat di dalamnya.

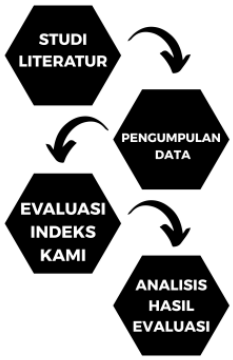
Evaluasi dilakukan menggunakan Indeks KAMI (Keamanan Informasi) versi 5.0 yang menekankan penilaian tingkat kematangan dan kesiapan penerapan standar ISO/IEC 27001:2022. Sebagai lembaga pengawas pemilu, BAWASLU memiliki karakteristik khusus dalam pengelolaan data sensitif dan peran strategis dalam menjaga integritas proses demokrasi. Oleh karena itu, penelitian ini memberikan nilai tambah melalui penerapan Indeks KAMI versi 5.0 pada konteks lembaga pengawas pemilu, serta analisis tingkat kematangan keamanan informasi dengan mempertimbangkan aspek perlindungan data pribadi dan keterlibatan pihak ketiga. Sejalan dengan perkembangan standar keamanan informasi tahun 2022, Indeks KAMI digunakan sebagai instrumen utama dalam proses evaluasi tata kelola keamanan informasi. (Imtikhan Azmi et al., 2024).

Evaluasi tingkat kesiapan penyelenggaraan layanan teknologi informasi pada BAWASLU ABC menggunakan Indeks Keamanan Informasi (KAMI) guna mendapatkan hasil tingkat kesiapan keamanan, kelengkapan, dan kematangan kerangka kerja keamanan informasi yang diterapkan. Hasil evaluasi diharapkan dapat menjadi perhatian bagi PSE sebagai pengelola teknologi informasi agar dapat berbenah serta melakukan perbaikan dan peningkatan keamanan informasi pada area-area yang dievaluasi, sesuai dengan standar SNI ISO/IEC 27001:2022 (Khusna and Sugiantoro, 2023).

2. METODE PENELITIAN

Kajian dilakukan dengan melalui metode deskriptif evaluatif yang menghasilkan *output* luaran menilai tingkat kesiapan, tata kelola dan kematangan penerapan keamanan informasi pada PSE (Akbar and Siregar, 2024; Karunia, Zahra and Amrozi, 2025). Pendekatan ini dimaksudkan untuk memberikan gambaran menyeluruh mengenai kondisi lapangan keamanan informasi sesuai dengan

hasil evaluasi menggunakan Indeks Keamanan Informasi (KAMI) yang diadopsi dengan standar ISO/IEC 27001:2022 (Gaba et al., 2023). Prosedur lengkap riset yang dilakukan secara keseluruhan terdapat pada Gambar 1.



Gambar 1. Prosedur Riset

2.1. Studi Literatur

Tahap studi literatur diselengarakan untuk meningkatkan potensi pemahaman terkait konsep, prinsip, serta kerangka kerja yang menjadi dasar dalam evaluasi keamanan informasi (Khusna and Sugiantoro, 2023). Fokus utama dalam studi ini adalah pada pedoman Indeks Keamanan Informasi (KAMI) yang disusun oleh Badan Siber dan Sandi Negara (BSSN) berfungsi sebagai media evaluasi tingkat kesiapan, tata kelola dan kematangan dalam implementasi keamanan informasi di Indonesia (Savitri et al., 2024). Selain itu, penelitian ini juga merujuk pada standar ISO/IEC 27001:2022, yang menjadi acuan global dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) (Wulansari and Novandi, 2022; Karunia, Zahra and Amrozi, 2025).

Melalui telaah literatur tersebut, diperoleh pemahaman konseptual mengenai aspek-aspek utama bidang keamanan informasi, terdiri atas tata kelola, pengelolaan risiko, kerangka kerja keamanan, pengelolaan aset, serta pengamanan teknologi (Clarissa and Wang, 2023; Fauzia Anis Sekar Ningrum et al., 2024). Studi ini juga meninjau hasil penelitian yang terdahulu yang menggunakan Indeks KAMI sebagai instrumen evaluasi, guna mengidentifikasi kesenjangan penelitian dan memperkuat landasan teoritis dalam pengembangan model analisis pada konteks organisasi yang diteliti (Dewantara and Sugiantoro, 2021; Paramita et al., 2022; Fauzia Anis Sekar Ningrum et al., 2024; Imtikhan Azmi et al., 2024).

2.2. Pengumpulan Data

Tahap pengumpulan data dilakukan untuk memperoleh informasi aktual terkait penerapan keamanan informasi pada organisasi (Imtikhan Azmi et al., 2024). Teknik pengumpulan data meliputi wawancara, observasi, dan pengkajian dokumen kerja yang relevan dengan aspek penilaian Indeks Keamanan Informasi (KAMI) (Akbar and Siregar, 2024). Wawancara dilakukan dengan pengelola teknologi informasi dan pihak terkait untuk memperoleh gambaran penerapan kebijakan keamanan informasi (Clarissa and Wang, 2023). Observasi digunakan untuk menilai kondisi nyata infrastruktur serta penerapan prosedur keamanan di lapangan, sedangkan kajian dokumen mencakup analisis terhadap kebijakan, pedoman, dan laporan internal organisasi (Ramadhani, Putra and Herlambang, 2020; Akbar and Siregar, 2024; Imtikhan Azmi et al., 2024). Data yang diperoleh selanjutnya dianalisis agar dapat disajikan ke dalam lima area utama Indeks KAMI guna evaluasi tingkat kesiapan dan kematangan pengelolaan keamanan informasi (Khusna and Sugiantoro, 2023; Habibullah, Nuruzzaman and Mulyanto, 2024).

2.3. Evaluasi Indeks KAMI

Taap proses evaluasi Indeks Keamanan Informasi (KAMI) pada penelitian ini diimplementasikan dari aplikasi Indeks KAMI versi 5.0 yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN). Versi terbaru ini dirancang untuk menilai tingkat kesiapan dan kematangan penerapan keamanan informasi pada organisasi PSE, serta diselaraskan dengan standar ISO/IEC 27001:2022 (BSSN, n.d.). Instrumen penilaian dalam Indeks KAMI 5.0 terdiri atas beberapa area utama menjadi fokus evaluasi. Area pertama tata kelola keamanan informasi, yang mencakup kebijakan, struktur di dalam organisasi serta mekanisme pengawasan dalam penerapan keamanan informasi. Area kedua pengelolaan risiko keamanan informasi, berfokus terhadap proses identifikasi, analisis, dan mitigasi risiko terhadap aset iformasi. Area ketiga kerangka kerja keamanan informasi, mengevaluasi pengembangan, penerapan, dan pemeliharaan kebijakan serta prosedur keamanan informasi. Area keempat, yakni pengelolaan aset informasi berkaitan dengan penerapan inventarisasi aset keamanan, klasifikasi dan perlindungan aset informasi. Terakhir, teknologi dan keamanan informasi, menekankan penerapan kontrol teknis, proteksi sistem, dan pemanfaatan teknologi untuk menjaga keamanan data pribadi, terintegrasi, serta optimasi ketersediaan informasi.

Disamping lima area prioritas utama tersebut, Indeks KAMI versi 5.0 mencakup dua komponen tambahan, yaitu Perlindungan Data Pribadi (PDP) dan Suplemen, yang berfungsi menilai kepatuhan terhadap perlindungan data pribadi serta keamanan layanan pihak ketiga dan infrastruktur awan (Imtikhan Azmi et al., 2024).

Instrumen Indeks KAMI versi 5.0 disusun untuk menilai tingkat kesiapan dan kelengkapan pengamanan informasi sesuai standar SNI ISO/IEC 27001:2022 (Karunia, Zahra and Amrozi, 2025).

Setiap area penilaian terdiri atas tiga tahap yang mencerminkan kematangan keamanan informasi: tahap (1) menggambarkan pembentukan kerangka kerja dasar, tahap (2) menunjukkan konsistensi dan efektivitas penerapan kontrol, dan tahap (3) menilai kemampuan peningkatan berkelanjutan (Khusna and Sugiantoro, 2023). Hasil penilaian digunakan untuk menentukan skor kategori pengamanan yang menggambarkan tingkat kesiapan keamanan informasi organisasi (Wijayanti et al., 2020; Imtikhan Azmi et al., 2024). Dalam penelitian ini, instrumen tersebut diterapkan pada BAWASLU ABC guna menilai dan menetapkan prioritas peningkatan pengamanan informasi secara menyeluruh. Nilai evaluasi skor tingkat pengamanan berdasarkan kondisi pengamanan disajikan pada Tabel 1.

Table 1. Skor Tingkat Kesiapan Berdasarkan Kategori Pengamanan

	Kategori Pengamanan		
StatusPengamanan	**1**	**2**	**3**
Tidak Dilakukan	0	0	0
Dalam Perenacanaan	1	2	3
Dalam Penerapan/Diterapkan Sebagaian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9
Tidak Berlaku /Relevan	0	0	0

Tabel 1 menunjukkan skor kategori pengamanan yang diperoleh dari hasil pengukuran setiap status penerapan pengamanan informasi (Imtikhan Azmi et al., 2024). Status penerapan pengamanan informasi diklasifikasi penilaian dibagi menjadi empat tingkat, yakni Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan atau Diterapkan Sebagian, serta Diterapkan Secara Menyeluruh, dengan bobot nilai 0, 1–3, 2–6, dan 3–9 sesuai kategori pengamanan. Status Tidak Berlaku/Relevan diberi nilai 0 bila tidak sesuai konteks. Penilaian mengacu pada pendekatan tingkat kematangan keamanan informasi berbasis kerangka COBIT dan *Capability Maturity Model Integration* (CMMI), pedekatan yang terdiri dari lima tingkat: I (Awal), II (Dasar), III (Terdefinisi dan Konsisten), IV (Terkelola dan Terukur), dan V (Optimal), dengan tambahan level antara I+ hingga IV+ agar mendapat tingkat kematangan antar level. Sesuai standar SNI ISO/IEC 27001:2022, tingkat kesiapan minimal yang diharapkan berada pada Tingkat III+, yang menandakan penerapan keamanan informasi telah berjalan secara konsisten dan terdokumentasi (R.Y Rahman, 2023; Imtikhan Azmi et al., 2024).

2.4. Analisis Hasil Evaluasi

Pada tahap akhir penelitian adalah analisis terhadap hasil evaluasi yang dilakukan terhadap penerapan keamanan informasi di BAWASLU ABC. Tahap ini bertujuan untuk menilai hasil temuan dengan Indeks KAMI versi 5.0, agar mendapatkan deskripsi tentang tingkat kesiapan keamanan informasi pada organisasi. Hasil analisis selanjutnya menjadi dasar dalam penyusunan kesimpulan serta dapat dijadikan bahan pertimbangan bagi pengelola Teknologi Informasi Komunikasi (TIK) di lingkungan BAWASLU ABC dalam meningkatkan tata kelola keamanan informasinya (Imtikhan Azmi et al., 2024; Savitri et al., 2024).

3. PEMBAHASAN

Bab ini memaparkan mengenai hasil temuan penelitian yang diperoleh melalui penerapan Indeks KAMI versi 5.0 sebagai instrumen evaluasi keamanan informasi. Agar dapat menilai tingkat kesiapan pengelolaan keamanan informasi pada BAWASLU ABC.

3.1. Kategori Sistem Elektronik

Kategori sistem elektronik dimaksudkan agar mengevaluasi tingkat klasifikasi sistem elektronik yang digunakan oleh organisasi (Clarissa and Wang, 2023). Kategori ini mencakup tiga tingkat ketergantungan, yaitu rendah, tinggi, dan strategis. Penilaian dilakukan melalui 10 butir pertanyaan yang menggambarkan karakteristik instansi atau organisasi yang dievaluasi. Berdasarkan hasil penilaian, diperoleh skor total sebesar 14, yang menempatkan sistem elektronik pada kategori dengan tingkat ketergantungan rendah. Berikut tiga kategori evaluasi ditampilkan dalam Tabel 2.

Table 2. Skor kategori sistem elektronik

Tingkat Ketergatungan TIK	Batas Bawah	Batas Atas	Klasifikasi
A	10	15	RENDAH
B	16	34	TINGGI
C	35	50	STRATEGIS

Berdasarkan hasil evaluasi, sistem elektronik pada BAWASLU ABC memperoleh skor 14 yang termasuk dalam kategori rendah. Artinya, ketergantungan terhadap sistem elektronik masih terbatas pada fungsi administrasi dan operasional, sehingga gangguan sistem tidak berdampak signifikan terhadap tugas utama organisasi. Hasil ini menjadi acuan awal untuk memperkuat kebijakan dan kontrol dasar keamanan informasi guna meningkatkan kesiapan serta pengelolaan TIK yang lebih andal dan berkelanjutan (Wulansari and Novandi, 2022). Maka, dapat disimpulkan bahwa tingkat ketergantungan TIK pada BAWASLU ABC berada pada kategori rendah.

3.2. Tata Kelola Keamanan Informasi

Kategori tata kelola keamanan informasi memiliki tujuan agar dapat menilai tingkat kesiapan organisasi yang memiliki fungsi, tugas, dan tanggung jawabnya terhadap pengelolaan keamanan informasi dalam organisasi (Paramita et al., 2022). Proses penilaian didasarkan pada empat standar

penerapan, meliputi tidak dilakukan, dalam tahap perencanaan, sedang diterapkan atau baru sebagian, dan telah diterapkan secara menyeluruh. Aspek ini terdiri atas 22 butir pertanyaan yang menilai peran serta mekanisme organisasi dalam menjaga keamanan informasi. Rincian pertanyaan mencakup 8 butir kategori pengamanan I dengan tingkat kematangan II, 5 butir kategori pengamanan II dengan tingkat kematangan II, 3 butir kategori pengamanan II dengan tingkat kematangan III, serta 6 butir kategori pengamanan III dengan tingkat kematangan IV. Hasil skor evaluasi pada aspek tata kelola keamanan informasi disajikan secara rinci pada Tabel 3 berikut ini.

Table 3. Skor Evaluasi Tata Kelola Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	8	24
2	8	48
3	6	54
Total	**22**	**126**

Dari hasil skor evaluasi, bagian Tata Kelola Keamanan Informasi mencatat skor total 126 berdasarkan 22 pertanyaan yang diklasifikasikan dalam tiga kategori pengamanan. Kategori pengamanan I dengan 8 pertanyaan memperoleh nilai 24, kategori pengamanan II dengan 8 pertanyaan memperoleh nilai 48, dan kategori pengamanan III dengan 6 pertanyaan memperoleh nilai 54. Berdasarkan hasil penilaian, tingkat kematangan keamanan informasi di BAWASLU ABC telah mencapai Tingkat I (Kondisi Awal), Tingkat II (Kerangka Dasar Diterapkan), serta Tingkat III (Terdefinisi dan Konsisten). Berdasarkan capaian tersebut, dapat disimpulkan bahwa area ini telah melampaui ambang batas tingkat kematangan minimal sebagai standar tata kelola keamanan informasi yang ditetapkan dalam SNI ISO/IEC 27001:2022, yaitu berada pada Tingkat III+, yang menandakan bahwa penerapan tata kelola keamanan informasi di BAWASLU ABC telah berjalan secara konsisten namun tetap memerlukan peningkatan level kematangan yang lebih tinggi dengan memperbaiki aspek tata kelola dan pengelolaan risiko keamanan informasi (Clarissa and Wang, 2023).

3.3. Pengelolaan Risiko Keamanan Informasi

Kategori pengelolaan risiko keamanan informasi digunakan untuk mengevaluasi kesiapan penerapan manajemen risiko yang menjadi dasar dalam pengembangan strategi keamanan informasi organisasi (Savitri et al., 2024). Proses penilaian didasarkan pada empat kategori penerapan, yaitu tidak dilakukan, dalam tahap perencanaan, sedang diterapkan atau baru sebagian, dan telah diterapkan secara menyeluruh. Terdapat 16 butir pertanyaan yang mengabarkan pengelolaan risiko keamanan informasi dalam organisasi. Rincian pertanyaan mencakup 10 butir kategori pengamanan I dengan tingkat kematangan II, 2 butir kategoti pengamanan II dengan tingkat kematangan III, 2 butir kategori pengamanan II dengan tingkat kematangan IV, 2 butir kategori pengamanan III dengan tingkat kematangan V. Hasil evaluasi untuk bagian tata kelola keamanan informasi disajikan secara rinci pada Tabel 4 berikut.

Table 4. Skor Evaluasi Pengelolaan Risiko Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	10	30
2	4	24
3	2	18
Total	**16**	**72**

Berdasarkan hasil rekapitulasi pada tabel, total skor yang diperoleh untuk bagian tata kelola keamanan informasi adalah 72 dari 16 pertanyaan yang terbagi dalam tiga kategori pengamanan. Kategori pengamanan 1 dengan 10 pertanyaan memperoleh nilai 30, kategori pengamanan 2 dengan 4 pertanyaan memperoleh nilai 24, dan kategori pengamanan 3 dengan 2 pertanyaan memperoleh nilai 18. Hasil ini menunjukkan bahwa tingkat penerapan tata kelola keamanan informasi pada BAWASLU ABC berada pada tingkat kematangan sedang, dengan sebagian besar kontrol keamanan telah diterapkan namun masih memerlukan peningkatan dalam konsistensi dan efektivitas pelaksanaannya agar mencapai standar optimal sesuai SNI ISO/IEC 27001:2022 (Habibullah, Nuruzzaman and Mulyanto, 2024).

3.4. Kerangka Kerja Pengelolaan Keamanan Informasi

Kategori kerangka kerja pengelolaan keamanan informasi digunakan untuk menilai sejauh mana kebijakan, prosedur, dan strategi keamanan informasi telah disusun dan siap diterapkan oleh organisasi (Imtikhan Azmi et al., 2024). Proses penilaian mengacu pada empat kategori penerapan, meliputi tidak dilakukan, dalam tahap perencanaan, sedang diterapkan atau baru sebagian, dan telah diterapkan secara menyeluruh. Area kerangka kerja keamanan informasi dibagi menjadi dua subkategori utama, yaitu: (1) penyusunan serta pengelolaan kebijakan dan prosedur keamanan informasi dengan 22 butir pertanyaan, dan (2) pengelolaan strategi serta program keamanan informasi yang terdiri atas 10 pertanyaan. Subkategori pertama menilai perencanaan dan penerapan kebijakan melalui kombinasi tingkat kematangan II hingga IV, sedangkan subkategori kedua menilai strategi dan program keamanan informasi dengan tingkat kematangan II hingga V. Secara keseluruhan, hasil evaluasi menunjukkan bahwa organisasi telah memiliki kerangka kerja keamanan informasi yang cukup matang dan terstruktur, sebagaimana ditunjukkan pada Tabel 5.

Table 5. Skor Evaluasi Kerangka Kerja Pengelolaan Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	12	36
2	11	66
3	10	90
Total	**33**	**192**

Hasil evaluasi pada kerangka kerja pengelolaan keamanan informasi menunjukkan skor total sebesar 192, yang dihitung dari 33 pertanyaan dan terbagi dalam tiga kategori pengamanan. Kategori pengamanan I dengan 12 pertanyaan memperoleh nilai 36, kategori pengamanan II dengan 11 pertanyaan memperoleh nilai 66, dan kategori pengamanan III dengan 10 pertanyaan memperoleh nilai 90. Temuan evaluasi memperlihatkan bahwa BAWASLU ABC telah mencapai Tingkat III (Terdefinisi dan Konsisten) dalam penerapan keamanan informasi, serta mulai menunjukkan peningkatan ke arah Tingkat IV (Terkelola dan Terukur) (Wijayanti et al., 2020). Secara keseluruhan, hasil evaluasi menunjukkan bahwa penerapan kerangka kerja pengelolaan keamanan informasi di BAWASLU ABC telah berjalan efektif dan diterapkan secara konsisten sesuai dengan standar yang berlaku, meskipun masih diperlukan peningkatan pada aspek pengukuran kinerja dan pengelolaan berkelanjutan untuk mencapai tingkat kematangan optimal sesuai SNI ISO/IEC 27001:2022 (Wulansari and Novandi, 2022).

3.5. Pengelolaan Aset Informasi

Kategori pengelolaan aset informasi digunakan untuk mengevaluasi kelengkapan dan efektivitas pengamanan aset organisasi, meliputi seluruh tahapan siklus penggunaannya seperti identifikasi, klasifikasi, pengendalian, serta perlindungan perangkat keras, perangkat lunak, data, dan jaringan. Penilaian dilaksanakan dengan mengacu pada empat tingkat penerapan, yakni tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, serta diterapkan secara menyeluruh sebagai dasar pengukuran tingkat efektivitas dan konsistensi penerapan keamanan informasi (Savitri et al., 2024). Kategori ini terdiri atas tiga subkategori utama, yaitu pengelolaan aset informasi yang mencakup 30 butir pertanyaan dengan tingkat kematangan II hingga III, pengamanan layanan infrastruktur awan (*cloud service*) yang terdiri atas 11 butir pertanyaan dengan tingkat kematangan III, serta pengamanan fisik yang mencakup 12 butir pertanyaan dengan tingkat kematangan II hingga III. Secara keseluruhan, hasil evaluasi menunjukkan bahwa organisasi telah memiliki pengelolaan aset informasi yang cukup baik dan terstruktur, dengan penerapan kontrol keamanan yang meliputi aspek teknis, digital, dan fisik, meskipun masih diperlukan peningkatan pada efektivitas pengawasan serta kebijakan penggunaan layanan berbasis awan agar sejalan dengan standar SNI ISO/IEC 27001:2022, sebagaimana ditunjukkan pada Tabel 6.

Table 6. Skor Evaluasi Pengelolaan Aset Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	27	81
2	19	114
3	7	63
Total	**53**	**258**

Berdasarkan hasil evaluasi pada bagian pengelolaan aset informasi, diperoleh total skor sebesar 258 dari 53 pertanyaan yang terbagi dalam tiga kategori pengamanan. Kategori pengamanan I dengan 27 pertanyaan memperoleh nilai 81, kategori pengamanan II dengan 19 pertanyaan memperoleh nilai 114, dan kategori pengamanan III dengan 7 pertanyaan memperoleh nilai 63. Skor ini menunjukkan bahwa tingkat kematangan pengelolaan aset informasi pada BAWASLU ABC telah mencapai Tingkat III (Terdefinisi dan Konsisten) menuju Tingkat IV (Terkelola dan Terukur). Hal ini menandakan bahwa pengelolaan aset informasi di organisasi telah dilakukan secara sistematis dan berkesinambungan, mencakup aspek inventarisasi, perlindungan aset, layanan berbasis awan, serta keamanan fisik (Imtikhan Azmi et al., 2024). Meskipun demikian, peningkatan tetap diperlukan dalam hal efektivitas kontrol keamanan dan evaluasi berkala agar pengelolaan aset informasi semakin selaras dengan standar SNI ISO/IEC 27001:2022 (Zhang et al., 2021).

3.6. Teknologi Keamanan Informasi

Kategori teknologi keamanan informasi digunakan untuk menilai sejauh mana teknologi yang diterapkan telah lengkap, konsisten, dan efektif dalam melindungi aset informasi yang dimiliki organisasi (Wijayanti et al., 2020). Proses penilaian mengacu pada lima kategori penerapan, yaitu tidak dilakukan, dalam tahap perencanaan, sedang diterapkan atau baru sebagian diterapkan, telah diterapkan secara menyeluruh, serta tidak relevan terhadap konteks organisasi. Bagian ini terdiri atas satu subkategori utama, yaitu pengamanan teknologi, yang mencakup 35 butir pertanyaan dengan tingkat kematangan I hingga IV. Evaluasi pada bagian ini menilai penerapan solusi teknologi keamanan oleh organisasi, meliputi pengendalian akses, pemantauan jaringan, perlindungan data, serta deteksi dan respons insiden. Secara umum, hasil ini menggambarkan kemampuan organisasi dalam mengimplementasikan teknologi keamanan yang efektif dan berkelanjutan untuk memperkuat tata kelola keamanan informasi. Rincian hasil evaluasi disajikan pada Tabel 7.

Table 7. Skor Evaluasi Teknologi Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	14	42
2	15	90
3	6	51
Total	**35**	**183**

Hasil evaluasi menunjukkan bahwa teknologi keamanan informasi memperoleh skor total 183 dari 35 butir pertanyaan yang mencakup tiga kategori pengamanan. Kategori pengamanan I dengan 14 pertanyaan memperoleh nilai 42, kategori pengamanan II dengan 15 pertanyaan memperoleh nilai 90, dan kategori pengamanan III dengan 6 pertanyaan memperoleh nilai 51. Temuan ini mengindikasikan bahwa penerapan teknologi keamanan informasi di BAWASLU ABC telah mencapai Tingkat III (Terdefinisi dan Konsisten) dan sedang berkembang ke arah Tingkat IV (Terkelola dan Terukur). Hal tersebut menandakan bahwa organisasi telah menerapkan teknologi keamanan informasi secara efektif, meliputi pengendalian akses, pemantauan jaringan, serta perlindungan data dan sistem (Zhang et al., 2021). Meskipun demikian, masih diperlukan peningkatan pada aspek integrasi sistem dan mekanisme deteksi insiden agar pengelolaan teknologi keamanan informasi dapat mencapai tingkat optimal sesuai SNI ISO/IEC 27001:2022 (Marican et al., 2023).

3.7. Perlindungan Data Pribadi

Kategori PDP digunakan untuk menilai sejauh mana kontrol keamanan diterapkan secara lengkap, konsisten, dan efektif dalam pengelolaan serta perlindungan data pribadi organisasi (Sun et al., 2022). Proses penilaian mengacu pada empat kategori penerapan, meliputi tidak dilakukan, dalam tahap perencanaan, dalam penerapan atau sebagian diterapkan, dan telah diterapkan secara menyeluruh. Aspek PDP mencakup 16 butir pertanyaan yang menilai sejauh mana organisasi menerapkan kebijakan dan mekanisme perlindungan data pribadi. Rincian pertanyaan meliputi 4 butir kategori pengamanan I dengan tingkat kematangan II, 2 butir kategori pengamanan II dengan tingkat kematangan II, dan 10 butir kategori pengamanan II dengan tingkat kematangan III. Secara keseluruhan, hasil evaluasi menunjukkan bahwa penerapan perlindungan data pribadi telah dilakukan dengan cukup baik, meskipun masih diperlukan peningkatan pada konsistensi pengendalian dan kepatuhan terhadap kebijakan keamanan data, sebagaimana ditampilkan pada Tabel 8.

Table 8. Skor Evaluasi Perlindungan Data Pribadi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	4	12
2	2	12
3	10	60
Total	**16**	**84**

Berdasarkan hasil evaluasi pada bagian PDP, diperoleh total skor sebesar 84 dari 16 pertanyaan yang terbagi dalam tiga kategori pengamanan. Kategori pengamanan I dengan 4 pertanyaan memperoleh nilai 12, kategori pengamanan II dengan 2 pertanyaan memperoleh nilai 12, dan kategori pengamanan III dengan 10 pertanyaan memperoleh nilai 60. Hasil ini menunjukkan bahwa tingkat kematangan penerapan perlindungan data pribadi pada BAWASLU ABC telah mencapai Tingkat III (Terdefinisi dan Konsisten) (Chan, Yang and Fan, 2021). Artinya, kebijakan dan mekanisme perlindungan data pribadi telah diterapkan secara cukup sistematis dan konsisten di lingkungan organisasi (Irfan et al., 2020). Namun, masih diperlukan penguatan pada aspek pengawasan, audit kepatuhan, serta peningkatan kesadaran pegawai terhadap pentingnya keamanan data pribadi agar dapat mencapai tingkat kematangan yang lebih tinggi sesuai SNI ISO/IEC 27001:2022 tentang Perlindungan Data Pribadi (Alkhazi et al., 2022).

3.8. Suplemen

Kategori suplemen berperan sebagai komponen akhir evaluasi yang menilai efektivitas penggunaan teknologi dan keterlibatan pihak ketiga dalam perlindungan aset informasi (Sugiarto and Suryanto, 2022). Penilaian dilakukan berdasarkan empat tingkat penerapan (tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh). Area ini terdiri atas satu kategori utama, yaitu pengamanan keterlibatan pihak ketiga, yang menilai pengelolaan risiko, kebijakan keamanan, dan keberlanjutan layanan, termasuk pengelolaan subkontraktor, aset, serta penanganan insiden. Secara keseluruhan, bagian suplemen memberikan gambaran mengenai sejauh mana BAWASLU ABC telah menerapkan kebijakan dan kontrol keamanan secara terpadu dalam kerja sama dengan pihak ketiga. Hasil temuan selengkapnya disajikan pada Tabel 9.

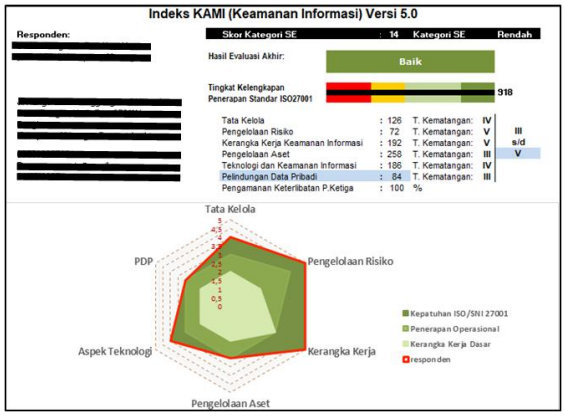
Table 9. Skor Evaluasi Suplemen

Kategori	Jumlah Pertanyaan	Nilai
1	27	3,00
Total	**27**	**100%**

Berdasarkan hasil evaluasi pada bagian suplemen, diperoleh total 27 pertanyaan dengan nilai rata-rata 3,00 atau tingkat pencapaian 100%. Temuan menunjukkan bahwa BAWASLU ABC telah melaksanakan pengamanan informasi dengan sangat baik pada aspek pengelolaan pihak ketiga, meliputi risiko, kebijakan keamanan, pengendalian aset, insiden, dan kelangsungan layanan. Nilai tersebut menandakan bahwa pengawasan terhadap pihak ketiga telah dijalankan secara konsisten, efektif, dan terdokumentasi dengan baik (Paramita et al., 2022). Secara umum, hasil ini menegaskan bahwa area suplemen telah mencapai tingkat kematangan tinggi sesuai SNI ISO/IEC 27001:2022, yang berkontribusi terhadap peningkatan berkelanjutan tata kelola keamanan informasi di BAWASLU ABC (Kawanishi et al., 2023).

Evaluasi kesiapan keamanan informasi BAWASLU ABC menggunakan Indeks KAMI versi 5.0 menunjukkan tingkat kematangan pada seluruh

area penilaian, termasuk tata kelola, risiko, kerangka kerja, aset, teknologi, perlindungan data pribadi, dan pengamanan pihak ketiga. Hasil ini memberikan gambaran umum tingkat kesiapan organisasi sesuai SNI ISO/IEC 27001:2022, serta menjadi dasar perencanaan strategi peningkatan keamanan informasi ke depan (Savitri et al., 2024). Gambar 2 menyajikan hasil evaluasi tingkat kematangan keamanan informasi berdasarkan area penilaian yang telah diukur.



Gambar 2. Dashboard Penilaian Indeks KAMI 5

Hasil evaluasi akhir menunjukkan bahwa BAWASLU ABC meraih skor 14 pada Kategori Sistem Elektronik (SE) dengan predikat rendah, serta skor total 918 dengan predikat “Baik”, menggambarkan penerapan standar ISO/IEC 27001 yang sesuai dengan kategori SE. Berdasarkan Gambar 2, terlihat fokus utama pada kepatuhan terhadap ISO/SNI 27001, pelaksanaan operasional, dan kerangka kerja keamanan informasi. Area dengan kinerja terbaik adalah kerangka kerja, pengelolaan risiko, teknologi, dan tata kelola, yang telah mencapai Tingkat IV (Terkelola dan Terukur). Secara keseluruhan, BAWASLU ABC telah menerapkan sistem keamanan informasi yang stabil, terukur, dan sejalan dengan standar internasional (Wulansari and Novandi, 2022).

Berdasarkan hasil evaluasi pada BAWASLU ABC, maka dilakukan perbandingan hasil evaluasi Indeks KAMI dengan beberapa instansi lain yang telah diteliti sebelumnya. Perbandingan ini bertujuan untuk mengetahui posisi tingkat kesiapan dan kematangan keamanan informasi BAWASLU ABC secara relatif terhadap organisasi sejenis. Hasil disajikan pada Tabel 10.

Table 10. Perbandingan Hasil Evaluasi

Institusi	Versi Indek KAMI	Skor Total	Tingkat Kematangan	Kategori
BAWASLU ABC	5.0	918	III-V	Baik
UIN Sunan Kalijaga	4.2	432	I+-II+	Tidak Layak
UPT-PSI UMK	4.2	480	II-III+	Cukup Baik
SMK XYZ	4.2	314	I-II	Tidak Layak

Berdasarkan dengan hasil perbandingan tingkat kesiapan keamanan informasi menggunakan Indeks KAMI, disumpulkan bahwa BAWASLU ABC memiliki tingkat kesiapan keamanan yang lebih tinggi dibandingkan dengan institusi lain. Hal ini terlihat dari skor yang didapatkan sebesar 918 dengan tingkat kematangan III-V masuk dalam kategori ”Baik”. Meskipun demikian masih perlunya optimasi peningkatan keamanan informasi ke arah yang optimal untuk seluruh aspek keamanan informasi.

4. KESIMPULAN

Berdasarkan hasil analisis dan evaluasi yang telah disampaikan pada bab sebelumnya, diperoleh kesimpulan sebagai berikut:

1. Hasil evaluasi menunjukkan bahwa BAWASLU ABC memperoleh skor 14 untuk Kategori Sistem Elektronik (SE) dengan predikat rendah, dan skor total 918 dengan predikat “Baik”, menggambarkan penerapan standar SNI ISO/IEC 27001:2022 sesuai dengan karakteristik kategori SE. Meskipun demikian, diperlukan peningkatan berkelanjutan untuk memastikan kesiapan keamanan informasi tetap adaptif terhadap perkembangan ancaman siber, khususnya melalui penguatan pengelolaan aset informasi, perlindungan data pribadi, serta mekanisme pengendalian risiko pada keterlibatan pihak ketiga, agar tingkat kematangan keamanan informasi dapat ditingkatkan secara menyeluruh dan berkelanjutan.
2. Berdasarkan hasil per area, BAWASLU ABC meraih skor: Tata Kelola Keamanan Informasi (126, Tingkat IV), Pengelolaan Risiko (72, Tingkat V), Kerangka Kerja Keamanan Informasi (192, Tingkat V), Pengelolaan Aset (258, Tingkat III), Teknologi dan Keamanan Informasi (186, Tingkat IV), Perlindungan Data Pribadi (86, Tingkat III), dan Pengamanan Keterlibatan Pihak Ketiga (100%).
3. Perbandingan utama penelitian ini dan sebelumnya terletak pada instrumen Indeks KAMI yang digunakan yakni dengan versi 5 dan mengkaji tentang kesiapan lembaga pengawas pemilu yang relatif sedikit terbatas dalam kajian sebelumnya. Perbedaan terlihat pada instumen penelitian terdahulu yang digunakan yakni dengan menggunakan versi 4.2 seperti yang tertera pada Tabel 10 memperlihatkan beragam lembaga dan institusi pendidikan, organisasi pemerintah dan non pemerintah, hal ini juga menunjukan kesiapan keamanan informasi pada lembaga strategis yang menangani data sensitif pada proses demokrasi. Hasil temuan menjadi rekomendasi penerapan Indeks KAMI versi 5.0 menjadi instrumen evaluasi yang mendasar bagi organisasi dalam mengukur kesiapan dan peningkatan keamanan informasi serta menjadi

acuan dalam menyusun kebijakan keamanan informasi yang lebih kompleks mengingat ancaman siber yang lebih modren dan adaktif.

DAFTAR PUSTAKA

Akbar, M.T. and *Siregar*, M.U., 2024. A Survey on Software Requirements Engineering in Information Technology Institutions. 9(2), pp.253–264.

Alkhazi, B., Alshaikh, M., Alkhezi, S. and Labbaci, H., 2022. Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, 10(November), pp.132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286.

BSSN, n.d. Konsultasi dan Assesment Indeks KAMI. [online] Available at: <https://www.bssn.go.id/indeks-kami/>.

Chan, C.C., Yang, C.Z. and Fan, C.F., 2021. Security Verification for Cyber-Physical Systems Using Model Checking. IEEE Access, 9, pp.75169–75186. https://doi.org/10.1109/ACCESS.2021.3081587.

Clarissa, S. and Wang, G., 2023. Assessing Information Security Management Using ISO 27001:2013. Jurnal Indonesia Sosial Teknologi, 4(9), pp.1361–1371. https://doi.org/10.59141/jist.v4i9.739.

Dewantara, R. and 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), p.1137. https://doi.org/10.25126/jtiik.2021863123.

Fauzia Anis Sekar Ningrum, Yudha Riwanto, Inggrid Yanuar Risca Pratiwi and Muhammad Ainul Fikri, 2024. Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI. Jurnal Informatika Polinema, 10(3), pp.437–444. https://doi.org/10.33795/jip.v10i3.5154.

Gaba, S., Budhiraja, I., Kumar, V., Martha, S., Khurmi, J., Singh, A., Singh, K.K., S.S.Askar and Abouhawwash, M., 2023. A Systematic analysis of enhancing Cyber Security using deep learning for Cyber Physical Systems. IEEE Access, 12(December 2023), pp.6017–6035. https://doi.org/10.1109/ACCESS.2023.3349022.

Green, J.M., Sarrafzadeh, A. and Anwar, M., 2025. Critique of Networked Election Systems: A Comprehensive Analysis of Vulnerabilities and Security Measures. Information, 17(1), p.10. https://doi.org/10.3390/info17010010.

Habibullah, R., Nuruzzaman, M.T. and Mulyanto, A., 2024. Evaluasi Keamanan Sistem Informasi Dengan Indeks KAMI Dan COBIT 5 Di Pesantren. Cyber Security dan Forensik Digital, 7(2), pp.69–80. https://doi.org/10.14421/csecurity.2024.7.2.4576.

Imtikhan Azmi, H., Tulus_akbar, Tasya Kumala Dewi, B. and Sugiantoro, B., 2024. Evaluasi Tingkat Kesiapan Keamanan Informasi Pada SMK XYZ Menggunakan Indeks KAMI Versi 4.2. Cyber Security dan Forensik Digital, 7(1), pp.42–49. https://doi.org/10.14421/csecurity.2024.7.1.4422.

Irfan, M., Hassan, M., Hassan, N., Habib, M., Khan, S. and Nasruddin, A.M., 2020. Project Management Maturity and Organizational Reputation: A Case Study of Public Sector Organizations. IEEE Access, 8, pp.73828–73842. https://doi.org/10.1109/ACCESS.2020.2988511.

Karunia, W.A., Zahra, A.F. and Amrozi, Y., 2025. 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 Digital*, 8(1), pp.10–16.

Kawanishi, Y., Nishihara, H., Yoshida, H., Yamamoto, H. and Inoue, H., 2023. A Study on Threat Analysis and Risk Assessment Based on the 'Asset Container' Method and CWSS. *IEEE Access*, 11(January), pp.18148–18156. https://doi.org/10.1109/ACCESS.2023.3246497.

Khusna, T.N. and Sugiantoro, B., 2023. Pengukuran Tingkat Keamanan Informasi Pada Upt-Psi Universitas Muria Kudus Berdasarkan Indeks Keamanan Informasi (Kami) Versi 4.2. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 8(3), pp.847–856. https://doi.org/10.29100/jipi.v8i3.3720.

Marican, M.N.Y., Razak, S.A., Selamat, A. and Othman, S.H., 2023. Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, 11(January), pp.5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766.

Nyoman Amie Sandrawati, 2024. ANTISIPASI CYBERCRIME DAN KESENJANGAN

DIGITAL DALAM PENERAPAN TIK DI KPU. pp.232–257.

Paramita, S., Siregar, S.A., Damanik, R.A. and ..., 2022. Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013. *Bulletin of Information …*, [online] 3(4), pp.374–379. Available at: <https://journal.fkpt.org/index.php/BIT/article/view/421%0Ahttps://journal.fkpt.org/index.php/BIT/article/download/421/263>.

R.Y Rahman, M.. H., 2023. EVALUASI KEAMANAN INFORMASI PADA SMAN 1 TANGGAMUS MENGGUNAKAN INDEKS KAMI VERSI 4.2. *JURNAL FASILKOM*, 13(2), pp.181–187.

Ramadhani, N.D., Putra, W.H.N. and Herlambang, A.D., 2020. Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, [online] 4(5), pp.1490–1498. Available at: <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7259>.

Savitri, R., Firmansyah, Dworo and Hasibuan, M.S., 2024. Information Security Measurement using INDEX KAMI at Metro City. *Journal of Applied Data Sciences*, 5(1), pp.33–45. https://doi.org/10.47738/jads.v5i1.152.

Sugiarto, P. and Suryanto, Y., 2022. Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index based on ISO 27001:2013. *International Journal of Mechanical Engineering*, 7(2), pp.974–5823.

Sun, N., Li, C.T., Chan, H., Dung Le, B., Islam, M.Z., Zhang, L.Y., Islam, M.R. and Armstrong, W., 2022. Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges. *IEEE Access*, 10, pp.44756–44777. https://doi.org/10.1109/ACCESS.2022.3168716.

Wijayanti, F., Sensuse, D.I., Putera, A.A. and Syahrizal, A., 2020. Assessment of Information Security Management System: A Case Study of Data Recovery Center in Ministry XYZ. *2020 3rd International Conference on Computer and Informatics Engineering, IC2IE 2020*, pp.393–398. https://doi.org/10.1109/IC2IE50715.2020.9274574.

Wulansari, T.T. and Novandi, D., 2022. Evaluation of Information Security Management Using the KAMI Index Framework. *2022 International Conference of Science and Information Technology in Smart Administration, ICSINTESA 2022*, (4), pp.173–177. https://doi.org/10.1109/ICSINTESA56431.2022.10041714.

Zhang, H., Pan, Y., Lu, Z., Wang, J. and Liu, Z., 2021. A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units. *IEEE Access*, 9, pp.149690–149706. https://doi.org/10.1109/ACCESS.2021.3124565.