Digital Research Transformation
Vol 2 No 2, 2026. p. 7-24.
E-ISSN : 3089-8684

Evaluasi Kesiapan Keamanan Informasi Dinas Sosial GHI Menggunakan Indeks KAMI 5.0

Adri Floren Timor.S[1], Teguh Kesuma Wiradana[2], Lily Indria[3], Hawari Alhaq[4], Muhammad Tulus Akbar[5]
Universitas Merangin, Jambi, Indonesia[1,2,3,4,5]
Email: adriflourentimors@gmail.com

ABSTRAK

Keamanan informasi merupakan aspek penting dalam mendukung keberlangsungan layanan dan perlindungan data pada Penyelenggara Sistem Elektronik (PSE). Penelitian ini bertujuan mengevaluasi kesiapan keamanan informasi Dinas Sosial GHI menggunakan Indeks KAMI Versi 5.0 yang mengacu pada SNI ISO/IEC 27001:2022. Metode yang digunakan adalah deskriptif evaluatif melalui wawancara dan observasi dokumen. Penilaian mencakup tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, teknologi keamanan informasi, pelindungan data pribadi, serta keterlibatan pihak ketiga. Hasil evaluasi menunjukkan Kategori Sistem Elektronik memperoleh skor 21 dengan kategori Tinggi, sedangkan skor kelengkapan keamanan informasi sebesar 170 dengan status Tidak Layak dan tingkat kematangan I–I+. Skor tiap area meliputi tata kelola 18, risiko 4, kerangka kerja 37, aset 52, teknologi 24, dan pelindungan data pribadi 35. Pengamanan pihak ketiga mencapai 10%. Hasil ini menunjukkan perlunya peningkatan terstruktur pada pengelolaan risiko, kebijakan keamanan, teknologi, pelindungan data pribadi, dan pihak ketiga secara berkelanjutan agar selaras dengan standar keamanan informasi yang berlaku.

Kata Kunci: Indeks KAMI 5.0, keamanan informasi, SNI ISO/IEC 27001:2022, pelindungan data pribadi.

ABSTRACT

Information security is essential for ensuring service continuity and data protection within Electronic System Providers (ESPs). This study evaluates the information security readiness of Dinas Sosial GHI using the KAMI Index Version 5.0 based on SNI ISO/IEC 27001:2022. A descriptive-evaluative method was applied through interviews and document observations. The assessment covered governance, risk management, security framework, asset management, information security technology, personal data protection, and third-party involvement. The results show that the Electronic System Category obtained a score of 21, classified as High, while the overall information security completeness score was 170, categorized as Not Feasible, with a maturity level of I–I+. The respective scores were governance 18, risk management 4, security framework 37, asset management 52, technology 24, and personal data protection 35. Third-party security achieved 10%. These findings indicate the need for structured improvements in risk management, security policies, technology, personal data protection, and third-party security.

Keywords: *KAMI Index 5.0, information security, SNI ISO/IEC 27001:2022, personal data protection.*

PENDAHULUAN

Perlindungan bidang keamanan informasi sangat penting untuk keberlangsungan operasional organisasi yang bergantung pada sistem digital karena kegagalan di bidang ini dapat menyebabkan kebocoran data dan gangguan layanan (Akbar, Veronica, et al., 2026). Akibatnya, penting untuk menjaga data dan seluruh komponen pendukungnya, termasuk sistem, jaringan, dan perangkat keras yang melakukan proses pengolahan, penyimpanan, dan penyebaran data (Akbar, Gussati, et al., 2026).

Meningkatnya kompleksitas dalam menjaga keamanan informasi disebabkan oleh kemajuan teknologi yang cepat. Ini terlihat dari meningkatnya jumlah serangan siber dengan tingkat kecanggihan serta dampak kerugian yang semakin besar (Fauzia Anis Sekar Ningrum et al., 2024). *Pishing*, *malware*, *ransomware*, dan eksploitasi celah keamanan perangkat lunak adalah ancaman yang masih belum sepenuhnya dapat diantisipasi oleh banyak organisasi, baik kecil maupun besar (Karunia et al., 2025). Kejahatan *cyber* biasanya menargetkan pelaku usaha kecil yang memiliki sistem keamanan lemah dan rentan terhadap serangan, sehingga para pembuat kebijakan harus memperhatikan masalah ini dalam konteks risiko bisnis (Imtikhan Azmi et al., 2024). Pada tahun 2022, tercatat 370,02 juta serangan siber di Indonesia, serangan ini mengalami peningkatatan yang sebelumnya hanya 266,74 juta jika dikalkulasikan peningkatan sebesar 38,72% (Bagaskara et al., 2025). Oleh sebab itu diperlukan peningkatan keamanan data dan kesalahan manusia dalam menyelengarakan informasi elektronik agar dapat melingdungi hak data pribadi (Akbar, Gussati, et al., 2026).

Menerapkan SMKI (Sistem Manajemen Keamanan Informasi) adalah salah satu cara untuk mencegah ancaman kejahatan siber. Ini terutama berlaku untuk institusi atau penyedia layanan informasi data publik yang sangat penting dan strategis (Imtikhan Azmi et al., 2024). Selain itu, SMKI membantu mengoptimalkan penggunaan sumber daya yang tersedia dan berfungsi sebagai panduan dalam pengendalian dan mitigasi berbagai risiko keamanan data (Akbar, Veronica, et al., 2026). Selain itu, untuk mengurangi risiko kerugian besar (Imtikhan Azmi et al., 2024).

Indeks Keamanan Informasi (KAMI) digunakan untuk mengukur standar keamanan informasi di Indonesia. KAMI berfungsi sebagai alat untuk menilai dan mengevaluasi tingkat kesiapan, kelengkapan, dan kematangan implementasi tata kelola keamanan informasi sesuai karakteristik yang tercantum dalam SNI ISO/IEC 27001 (Akbar, Veronica, et al., 2026; Imtikhan Azmi et al., 2024). Berbagai organisasi Penyelengara Sistem Elektronik (PSE), baik pemerintah maupun non-pemerintah, akan menggunakan Evaluasi Indeks KAMI untuk menilai kematangan manajemen keamanan layanan informasi digital (Dewantara & Sugiantoro, 2021).

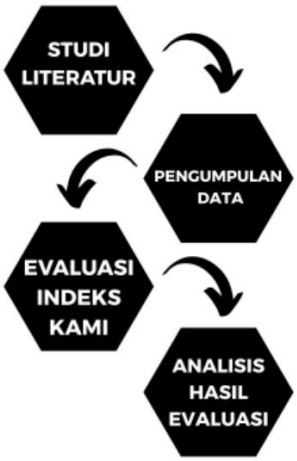
Untuk mengevaluasi kesiapan keamanan informasi di berbagai lembaga publik dan pemerintah, banyak penelitian telah menggunakan model evaluasi Indeks KAMI versi 4.2, yang berbasis ISO/IEC 27001:2013 dan digunakan secara luas oleh organisasi PSE. Ini menyediakan referensi dan pola evaluasi yang mapan (Imtikhan Azmi et al., 2024). Namun, 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, dan aspek privasi data, seiring dengan meningkatnya kompleksitas ancaman siber dan kebutuhan perlindungan data pribadi (Fauzia Anis Sekar Ningrum et al., 2024).

Tujuan dari penelitian ini adalah untuk mengukur tingkat kesiapan untuk keamanan informasi dan penerapan tata kelola keamanan pada organisasi PSE (Penyelenggara Sistem Elektronik), yaitu Dinas Sosial GHI tingkat kabupaten. Nama organisasi disamarkan untuk menjaga data lembaga tetap rahasia.

Indeks KAMI (Keamanan Informasi) versi 5.0 digunakan untuk melakukan evaluasi, yang menekankan tingkat kematangan dan kesiapan untuk menerapkan standar ISO/IEC 27001:2022. Sebagai lembaga pemerintah, Dinas Sosial GHI memiliki fitur khusus dalam pengelolaan data sensitif dan peran strategis dalam menjaga integritas data. Oleh karena itu, penelitian ini meningkatkan nilai melalui penerapan Indeks KAMI versi 5.0 dalam konteks pemerintahan dan menganalisis tingkat kematangan keamanan data dengan mempertimbangkan elemen perlindungan data pribadi dan keterlibatan pihak ketiga. Indeks KAMI digunakan sebagai alat utama dalam proses evaluasi tata kelola keamanan data seiring dengan perkembangan standar keamanan data pada tahun 2022 (Akbar, Veronica, et al., 2026).

METODE PENELITIAN

Untuk melakukan penelitian ini, menggunakan pendekatan deskriptif evaluasi yang digunakan. Hasil luaran dari pendekatan ini menunjukkan tingkat kesiapan, manajemen, dan kematangan implementasi keamanan informasi pada PSE (Akbar, Veronica, et al., 2026; Akbar & Siregar, 2024; Imtikhan Azmi et al., 2024; Karunia et al., 2025). Metode ini bertujuan untuk memberikan gambaran mendalam tentang situasi keamanan informasi di bidang ini sesuai dengan evaluasi yang dilakukan menggunakan Indeks Keamanan Informasi (KAMI), yang ditetapkan sesuai dengan ISO/IEC 27001:2022 (Akbar, Gussati, et al., 2026). Gambar 1 menunjukkan proses riset yang dilakukan secara keseluruhan.



Gambar 1. Prosedur Riset

Salah satu tujuan dari tahap studi literatur adalah untuk meningkatkan peluang untuk memahami konsep, prinsip, dan struktur yang menjadi dasar dari evaluasi keamanan informasi (Khusna & Sugiantoro, 2023). Indeks Keamanan Informasi (KAMI), yang dibuat oleh Badan Siber dan Sandi Negara (BSSN), adalah subjek utama

penelitian ini. KAMI dibuat untuk menilai kesiapan, tata kelola, dan kematangan implementasi keamanan informasi di Indonesia (Akbar, Veronica, et al., 2026). Selain itu, studi ini mengacu pada standar ISO/IEC 27001:2022, yang berfungsi sebagai standar internasional untuk penerapan Sistem Manajemen Keamanan Informasi (SMKI) (Imtikhan Azmi et al., 2024; Karunia et al., 2025).

Dengan membaca literatur tersebut, kita dapat memperoleh pemahaman konseptual tentang hal-hal seperti tata kelola, pengelolaan risiko, kerangka kerja keamanan, pengelolaan aset, dan pengamanan teknologi (Akbar, Veronica, et al., 2026; Fauzia Anis Sekar Ningrum et al., 2024). Selain itu, penelitian ini meninjau temuan penelitian sebelumnya yang menggunakan Indeks KAMI sebagai alat evaluasi. Tujuan dari penelitian ini adalah untuk mengidentifikasi perbedaan dalam hasil penelitian dan untuk memperkuat fondasi teoritis untuk mengembangkan model analisis yang sesuai dengan konteks organisasi yang diteliti (Akbar, Veronica, et al., 2026; Fauzia Anis Sekar Ningrum et al., 2024; Imtikhan Azmi et al., 2024).

Tahap pengumpulan data dilakukan untuk mendapatkan informasi yang relevan tentang praktik keamanan data organisasi (Akbar, Gussati, et al., 2026). Metode pengumpulan data termasuk observasi, wawancara, dan pemeriksaan dokumen kerja terkait aspek penilaian Indeks Keamanan Informasi (KAMI) (Akbar & Siregar, 2024). Untuk mendapatkan gambaran tentang implementasi kebijakan keamanan informasi, pengelola teknologi informasi dan pihak terkait diwawancarai (Clarissa & Wang, 2023). Kajian dokumen mencakup analisis kebijakan, pedoman, dan laporan internal organisasi, sedangkan observasi digunakan untuk menilai kondisi nyata infrastruktur dan penerapan prosedur keamanan di lapangan (Akbar & Siregar, 2024; Imtikhan Azmi et al., 2024). Selanjutnya, data yang diperoleh dianalisis dan disajikan dalam lima area utama Indeks KAMI. Ini dilakukan untuk mengevaluasi tingkat kesiapan dan kematangan dalam pengelolaan keamanan data (Habibullah et al., 2024).

Penelitian ini menggunakan aplikasi Indeks Keamanan Informasi (KAMI) versi 5.0, yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN). Versi terbaru ini dibuat untuk memenuhi standar ISO/IEC 27001:2022 dan menilai kematangan dan kesiapan penerapan keamanan informasi pada organisasi PSE (Akbar, Veronica, et al., 2026). Alat penilaian Indeks KAMI 5.0 terdiri dari beberapa topik utama yang menjadi fokus penilaian. Tata kelola keamanan informasi terdiri dari empat area. Area pertama adalah tata kelola keamanan informasi, yang mencakup peraturan, struktur organisasi, dan mekanisme pengawasan dalam penerapan keamanan informasi. Area kedua adalah pengelolaan risiko keamanan informasi, yang berfokus pada proses identifikasi, analisis, dan pengurangan risiko terhadap aset informasi. Area ketiga adalah kerangka kerja keamanan informasi, yang meninjau pengembangan, penerapan, dan pemeliharaan kebijakan dan prosedur keamanan informasi. Area keempat adalah tata kelola Terakhir, teknologi dan keamanan informasi berfokus pada penggunaan kontrol teknis, perlindungan sistem, dan teknologi untuk memastikan keamanan, integrasi, dan ketersediaan data pribadi (Akbar, Gussati, et al., 2026; Akbar, Veronica, et al., 2026; Imtikhan Azmi et al., 2024).

Indeks KAMI versi 5.0 juga mencakup dua komponen tambahan selain lima area prioritas utama tersebut, ini adalah Perlindungan Data Pribadi (PDP) dan Suplemen.

Kedua komponen ini berfungsi untuk menilai kepatuhan terhadap perlindungan data pribadi serta keamanan layanan pihak ketiga dan infrastruktur awan (Akbar, Gussati, et al., 2026).

Instrumen Indeks KAMI versi 5.0 dibuat untuk menilai kesiapan dan kelengkapan sistem pengamanan informasi sesuai dengan standar SNI ISO/IEC 27001:2022 (Karunia et al., 2025). Setiap bidang penilaian terdiri dari tiga tahap yang menunjukkan kematangan keamanan informasi. Tahap pertama menunjukkan pembentukan kerangka kerja dasar, tahap kedua menunjukkan betapa efektif dan konsisten penerapan kontrol, dan tahap ketiga menilai potensi peningkatan berkelanjutan (Khusna & Sugiantoro, 2023). Hasil penilaian digunakan untuk membuat kategori pengamanan, yang menunjukkan seberapa siap suatu organisasi untuk melindungi informasinya (Akbar, Gussati, et al., 2026; Akbar, Veronica, et al., 2026; Imtikhan Azmi et al., 2024). Instrumen ini diterapkan pada Dinas Sosial GHI dalam penelitian ini untuk menilai dan menetapkan prioritas untuk peningkatan pengamanan informasi secara keseluruhan. Tabel 1 menunjukkan nilai evaluasi tingkat pengamanan berdasarkan kondisi pengamanan.

Tabel 1. Skor Kesiapan Berdasarkan Kategori Keamanan

	Kategori Pengamanan		
Status Pengamanan	1	**2**	**3**
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan/Diterapkan Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9
Tidak Berlaku/Relevan	0	0	0

Tabel 1 menunjukkan skor kategori pengamanan berdasarkan hasil pengukuran untuk setiap status penerapan pengamanan informasi (Imtikhan Azmi et al., 2024). Skor penilaian dibagi menjadi empat kategori: Tidak Dilakukan, Dalam Perencanaan, Dalam Penerapan atau Diterapkan Sebagian, dan Diterapkan Secara Menyeluruh. Status Tidak Berlaku/Relevan diberi skor 0, 1–3, 2–6, dan 3–9. Sesuai dengan standar SNI ISO/IEC 27001:2022, tingkat kesiapan minimal yang diharapkan dalam tingkat kematangan keamanan informasi adalah pada tingkat I (Awal), II (Dasar), III (Terdefinisi dan Konsisten), IV (Terkelola dan Terukur), dan V (Optimal). Pendekatan tingkat kematangan keamanan informasi ini didasarkan pada kerangka COBIT dan Model *Capability Maturity Model Integration* (CMMI) (Akbar, Gussati, et al., 2026; Akbar, Veronica, et al., 2026; R.Y Rahman, 2023).

Akhir dari penelitian adalah menilai hasil evaluasi keamanan data di Dinas Sosial GHI. Tujuan dari tahap ini adalah untuk mengevaluasi hasil dengan Indeks KAMI versi 5.0, memberikan gambaran tentang seberapa siap organisasi untuk melindungi data pribadi mereka. Hasil analisis selanjutnya dapat digunakan sebagai dasar untuk penyusunan kesimpulan dan dapat digunakan oleh pengelola Teknologi Informasi Komunikasi (TIK) di Dinas Sosial GHI untuk meningkatkan tata kelola keamanan informasi mereka (Akbar, Veronica, et al., 2026).

PEMBAHASAN

Untuk menilai kesiapan pengelolaan keamanan informasi Dinas Sosial GHI, bab ini memaparkan hasil penelitian yang dilakukan dengan menggunakan Indeks KAMI versi 5.0 sebagai alat evaluasi keamanan informasi.

Kategori Sistem Elektronik

Kategori sistem elektronik dibuat untuk mengevaluasi tingkat klasifikasi sistem elektronik yang digunakan oleh organisasi (Clarissa & Wang, 2023). Ada tiga tingkat ketergantungan: strategis, tinggi, dan rendah. Proses penilaian terdiri dari sepuluh pertanyaan yang menjelaskan fitur organisasi atau instansi yang dievaluasi. Hasil penilaian menunjukkan bahwa sistem elektronik berada dalam kategori dengan tingkat ketergantungan rendah, dengan skor total sebesar 14. Tabel 2 menunjukkan tiga kategori evaluasi.

Tabel 2. Skor Kategori Sistem Elektronik

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

Hasil penilaian menunjukkan bahwa sistem elektronik pada Dinas Sosial GHI memperoleh skor sebesar 21 dan termasuk dalam kategori tinggi. Temuan ini menunjukkan bahwa keberadaan sistem elektronik memiliki peran yang cukup penting dalam mendukung pelaksanaan proses administrasi dan operasional organisasi. Meskipun belum sepenuhnya menjadi penentu keberlangsungan seluruh proses bisnis utama, gangguan atau kegagalan pada sistem elektronik berpotensi memengaruhi efektivitas dan efisiensi pelayanan serta aktivitas operasional organisasi. Oleh karena itu, hasil penilaian ini dapat dijadikan dasar bagi Dinas Sosial GHI untuk memperkuat kebijakan, tata kelola, serta kontrol keamanan informasi guna meningkatkan kesiapan organisasi dalam menghadapi risiko keamanan informasi dan mendukung pengelolaan teknologi informasi dan komunikasi (TIK) yang lebih baik dan berkelanjutan (Bakhtiar & Salsabila Hidayat, 2023). Dengan demikian, dapat disimpulkan bahwa Dinas Sosial GHI memiliki tingkat ketergantungan yang cukup tinggi terhadap pemanfaatan TIK dalam mendukung aktivitas organisasi.

Tata Kelola Keamanan Informasi

Tujuan dari kategori tata kelola keamanan informasi adalah untuk menentukan seberapa siap sebuah organisasi untuk mengelola keamanan informasi. Kategori ini dibentuk untuk menentukan siapa yang bertanggung jawab atas fungsi, tugas, dan tanggung jawab yang terkait dengan pengelolaan keamanan informasi dalam organisasi (Paramita et al., 2022). Proses penilaian didasarkan pada empat standar penerapan: tidak dilakukan, dalam tahap perencanaan, sedang diterapkan atau baru sebagian, dan telah diterapkan secara keseluruhan. Aspek ini terdiri dari dua puluh dua pertanyaan yang

menilai fungsi dan cara organisasi menjaga keamanan data. Tabel 3 berikut menunjukkan hasil evaluasi aspek tata kelola keamanan informasi. Pertanyaan yang diberikan 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, dan 6 butir kategori pengamanan III dengan tingkat kematangan IV.

Tabel 3. Skor Evaluasi Tata Kelola Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	8	8
2	8	10
3	6	0
Total	**22**	**18**

Dari hasil skor evaluasi, bagian Tata Kelola Keamanan Informasi mencatat skor total 18 berdasarkan 22 pertanyaan yang diklasifikasikan ke dalam tiga kategori pengamanan. Kategori Pengamanan I yang terdiri atas 8 pertanyaan memperoleh nilai 8, Kategori Pengamanan II yang terdiri atas 8 pertanyaan memperoleh nilai 10, sedangkan Kategori Pengamanan III yang terdiri atas 6 pertanyaan memperoleh nilai 0. Berdasarkan hasil penilaian tersebut, tingkat kematangan keamanan informasi di Dinas Sosial GHI masih menunjukkan capaian yang relatif rendah, terutama pada Kategori Pengamanan III yang belum memperoleh nilai. Kondisi ini menunjukkan bahwa penerapan tata kelola keamanan informasi belum sepenuhnya mencapai tingkat kematangan yang memadai dan masih memerlukan peningkatan pada sejumlah aspek. Oleh karena itu, Dinas Sosial GHI perlu melakukan penguatan terhadap penerapan tata kelola keamanan informasi, khususnya melalui penyempurnaan kebijakan dan prosedur, peningkatan konsistensi implementasi pengamanan, serta penguatan pengelolaan risiko keamanan informasi agar dapat mencapai tingkat kematangan yang lebih tinggi dan selaras dengan standar SNI ISO/IEC 27001:2022 (Clarissa & Wang, 2023).

Pengelolaan Risiko Keamanan Informasi Kategori

Mengelola risiko keamanan informasi adalah kategori yang digunakan untuk mengevaluasi seberapa siap organisasi untuk menerapkan manajemen risiko, yang merupakan bagian penting dari strategi keamanan informasi organisasi (Akbar, Gussati, et al., 2026). Dalam proses penilaian, ada empat jenis penerapan: tidak dilakukan, dalam tahap perencanaan, sedang diterapkan atau baru sebagian, dan telah diterapkan secara keseluruhan. Pengelolaan risiko keamanan data organisasi dibahas dalam enam belas pertanyaan. Tabel 4 berikut menyajikan hasil evaluasi bagian manajemen keamanan informasi secara rinci, yang mencakup sepuluh kategori pengamanan I dengan tingkat kematangan II, dua kategori pengamanan II dengan tingkat kematangan III, dua kategori pengamanan III dengan tingkat kematangan IV, dan dua kategori pengamanan III dengan tingkat kematangan V.

Tabel 4. Skor Evaluasi Pengelolaan Risiko Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai

1	10	4
2	4	0
3	2	0
Total	**16**	**4**

Berdasarkan hasil rekapitulasi pada tabel, total skor yang diperoleh untuk bagian Tata Kelola Keamanan Informasi adalah 4 dari 16 pertanyaan yang terbagi ke dalam tiga kategori pengamanan. Kategori Pengamanan 1 yang terdiri atas 10 pertanyaan memperoleh nilai 4, sedangkan Kategori Pengamanan 2 yang terdiri atas 4 pertanyaan dan Kategori Pengamanan 3 yang terdiri atas 2 pertanyaan masing-masing memperoleh nilai 0. Hasil ini menunjukkan bahwa tingkat penerapan tata kelola keamanan informasi pada Dinas Sosial GHI masih berada pada tahap awal dan belum diterapkan secara optimal. Rendahnya skor yang diperoleh, khususnya belum adanya nilai pada Kategori Pengamanan 2 dan 3, menunjukkan bahwa masih terdapat berbagai aspek tata kelola keamanan informasi yang perlu dikembangkan dan diterapkan secara lebih sistematis. Oleh karena itu, Dinas Sosial GHI perlu melakukan peningkatan secara menyeluruh terhadap kebijakan, prosedur, pembagian tanggung jawab, serta implementasi kontrol keamanan informasi agar tingkat kematangannya dapat meningkat dan penerapannya semakin selaras dengan SNI ISO/IEC 27001:2022 (Habibullah et al., 2024).

Kerangka Kerja Pengelolaan Keamanan Informasi

Dengan menggunakan kategori kerangka kerja pengelolaan keamanan informasi, organisasi dapat menilai seberapa baik kebijakan, prosedur, dan strategi keamanan informasi telah dibuat dan siap diterapkan (Imtikhan Azmi et al., 2024). Dalam proses evaluasi, ada empat jenis penerapan yang berbeda: tidak dilakukan, dalam tahap perencanaan, sedang diterapkan atau baru diterapkan, dan telah diterapkan secara keseluruhan. Dua subkategori utama membagi area kerangka kerja keamanan informasi: (1) penyusunan dan pengelolaan kebijakan dan prosedur keamanan informasi dengan 22 pertanyaan, dan (2) pengelolaan strategi dan program keamanan informasi dengan 10 pertanyaan. Subkategori pertama menilai perencanaan dan penerapan kebijakan dengan menggunakan kombinasi tingkat kematangan II hingga IV. Subkategori kedua menilai strategi dan program keamanan informasi dengan menggunakan kombinasi tingkat kematangan I hingga IV.

Tabel 5. Skor Evaluasi Kerangka Kerja Pengelolaan Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	12	14
2	11	20
3	10	3
Total	**33**	**37**

Hasil evaluasi pada Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi menunjukkan bahwa Dinas Sosial GHI memperoleh total nilai evaluasi sebesar 37. Penilaian dilakukan terhadap 33 pertanyaan yang terbagi ke dalam tiga tahap penerapan, yaitu 12 pertanyaan pada Tahap I, 11 pertanyaan pada Tahap II, dan 10 pertanyaan pada Tahap III. Pada Tahap I diperoleh total skor sebesar 17, sedangkan

akumulasi skor Tahap I dan Tahap II mencapai 37. Meskipun akumulasi tersebut memenuhi kriteria penilaian Tahap I dan II, penilaian pada Tahap III dinyatakan tidak valid karena belum memenuhi batas skor minimum sebesar 68. Berdasarkan penilaian tingkat kematangan, Dinas Sosial GHI memperoleh skor 16 pada Tingkat Kematangan II, yang telah melampaui skor minimum sebesar 15, tetapi masih berada di bawah skor pencapaian sebesar 24. Dengan demikian, status kematangan kerangka kerja pengelolaan keamanan informasi Dinas Sosial GHI berada pada Tingkat I+, yang menunjukkan bahwa penerapan pengelolaan keamanan informasi masih berada pada tahap awal pengembangan dan belum sepenuhnya memenuhi kriteria Tingkat II.

Hasil evaluasi juga menunjukkan bahwa beberapa aspek telah diterapkan secara menyeluruh, terutama pada strategi penerapan keamanan informasi, strategi penggunaan teknologi keamanan informasi, pelaksanaan program keamanan informasi, serta kegiatan audit internal dan evaluasinya. Namun, masih terdapat sejumlah aspek yang belum diterapkan atau masih dalam tahap perencanaan, khususnya terkait pengelolaan kebijakan dan prosedur keamanan informasi, *security patch*, *Secure Software Development Life Cycle* (*Secure SDLC*), *threat intelligence*, *business continuity planning*, *disaster recovery plan*, serta program peningkatan keamanan informasi jangka menengah dan panjang. Oleh karena itu, secara keseluruhan kerangka kerja pengelolaan keamanan informasi di Dinas Sosial GHI masih memerlukan peningkatan secara sistematis, terutama dalam penyusunan dan formalisasi kebijakan, penerapan prosedur keamanan, pengelolaan risiko, kesinambungan layanan, serta kegiatan pemantauan dan evaluasi berkelanjutan agar tingkat kematangan keamanan informasi dapat meningkat dan semakin selaras dengan prinsip pengelolaan keamanan informasi berdasarkan SNI ISO/IEC 27001:2022 (Akbar, Gussati, et al., 2026; Akbar, Veronica, et al., 2026).

Pengelolaan Aset Informasi Kategori

Kategori pengelolaan aset informasi mencakup seluruh tahapan siklus penggunaannya, seperti identifikasi, klasifikasi, pengendalian, dan perlindungan perangkat keras, perangkat lunak, data, dan jaringan. Ini digunakan untuk mengevaluasi kelengkapan dan efektivitas pengamanan aset organisasi. Ada empat tingkat penerapan yang digunakan dalam penilaian keamanan informasi: tidak dilakukan, dalam perencanaan, dalam penerapan, atau diterapkan sebagian. Penilaian ini digunakan sebagai dasar untuk mengukur seberapa efektif dan konsisten penerapan keamanan informasi (Akbar, Veronica, et al., 2026). Secara keseluruhan, kategori ini terdiri dari tiga subkategori utama: pengelolaan aset informasi, yang terdiri dari 30 pertanyaan dengan tingkat kematangan II hingga III, pengamanan layanan infrastruktur awan (*cloud service*), yang terdiri dari 11 pertanyaan dengan tingkat kematangan III, dan pengamanan fisik, yang terdiri dari 12 pertanyaan dengan tingkat kematangan II hingga III. Secara keseluruhan, hasil evaluasi menunjukkan bahwa organisasi memiliki pengelolaan aset sejalan dengan standar SNI ISO/IEC 27001:2022, sebagaimana ditunjukkan pada Tabel 6.

Tabel 6. Skor Evaluasi Pengelolaan Aset Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai

1	27	28
2	19	24
3	7	0
Total	**53**	**52**

Berdasarkan hasil evaluasi pada bagian Pengelolaan Aset Informasi, Dinas Sosial GHI memperoleh total nilai evaluasi sebesar 52 dari 53 pertanyaan yang mencakup pengelolaan aset informasi, pengamanan layanan infrastruktur awan (*cloud service*), dan pengamanan fisik. Dari keseluruhan pertanyaan tersebut, sebanyak 33 kontrol berada dalam tahap perencanaan, 5 kontrol telah diterapkan sebagian, dan 15 kontrol belum dilakukan. Hasil ini menunjukkan bahwa penerapan pengelolaan aset informasi di Dinas Sosial GHI masih berada pada tahap awal pengembangan dan belum dapat dikategorikan sebagai pengelolaan yang terdefinisi dan diterapkan secara konsisten. Beberapa kontrol telah mulai diterapkan, antara lain tata tertib penggunaan komputer, email, internet dan intranet, peraturan instalasi perangkat lunak, pengamanan fasilitas fisik, pemantauan infrastruktur melalui CCTV, serta pengamanan perangkat komputasi yang digunakan di luar lokasi kerja. Namun, sebagian besar aspek penting masih berada dalam tahap perencanaan, termasuk inventarisasi dan klasifikasi aset informasi, pengelolaan hak akses, prosedur pencadangan dan pemulihan data, pengelolaan perubahan dan konfigurasi, serta perlindungan terhadap infrastruktur teknologi informasi.

Pada aspek pengamanan layanan infrastruktur awan, penerapan kontrol juga masih terbatas. Beberapa kegiatan, seperti kajian risiko penggunaan layanan *cloud*, penetapan jenis data yang dapat disimpan atau diproses melalui layanan *cloud*, perlindungan data pribadi, dan evaluasi reputasi penyedia layanan masih berada dalam tahap perencanaan. Sementara itu, sejumlah kontrol penting, seperti pembagian tanggung jawab keamanan dengan penyedia layanan, aspek hukum penggunaan *cloud*, standar keamanan teknis, evaluasi kelayakan dan sertifikasi layanan, pelaporan insiden, serta strategi penghentian atau penggantian layanan *cloud* belum diterapkan. Kondisi serupa terlihat pada aspek pengamanan fisik, di mana sebagian besar kontrol masih dalam tahap perencanaan dan baru beberapa kontrol yang diterapkan sebagian. Dengan demikian, hasil evaluasi menunjukkan bahwa pengelolaan aset informasi pada Dinas Sosial GHI masih memerlukan peningkatan yang signifikan, terutama dalam hal formalisasi kebijakan dan prosedur, inventarisasi serta klasifikasi aset, pengelolaan akses, keamanan layanan *cloud*, pencadangan dan pemulihan data, serta pengamanan fisik. Peningkatan tersebut diperlukan agar pengelolaan aset informasi dapat diterapkan secara lebih menyeluruh, konsisten, dan selaras dengan prinsip keamanan informasi dalam SNI ISO/IEC 27001:2022 (Akbar, Gussati, et al., 2026; Imtikhan Azmi et al., 2024; Zhang et al., 2021).

Teknologi Keamanan Informasi

Kategori teknologi keamanan informasi digunakan untuk mengevaluasi tingkat kelengkapan, konsistensi, dan efektivitas penerapan teknologi dalam melindungi aset informasi organisasi (Akbar, Veronica, et al., 2026). Penilaian dilakukan berdasarkan lima status penerapan, yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, diterapkan secara menyeluruh, serta tidak relevan dengan kondisi

organisasi. Pada bagian ini terdapat satu subkategori utama, yaitu pengamanan teknologi, yang terdiri atas 35 butir pertanyaan dengan cakupan tingkat kematangan I sampai dengan IV. Evaluasi difokuskan pada sejauh mana organisasi telah menerapkan berbagai solusi teknologi keamanan, seperti pengendalian akses, pemantauan jaringan, perlindungan data, serta mekanisme deteksi dan penanganan insiden keamanan informasi. Hasil penilaian pada bagian ini memberikan gambaran mengenai kemampuan organisasi dalam memanfaatkan teknologi keamanan secara efektif, konsisten, dan berkelanjutan sebagai bagian dari upaya memperkuat tata kelola keamanan informasi. Rincian hasil evaluasi teknologi keamanan informasi disajikan pada Tabel 7.

Tabel 7. Skor Evaluasi Teknologi Keamanan Informasi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	14	7
2	15	8
3	6	9
Total	**35**	**24**

Hasil evaluasi pada aspek teknologi keamanan informasi menunjukkan bahwa Dinas Sosial GHI memperoleh total skor sebesar 24 dari 35 butir pertanyaan yang terbagi ke dalam tiga kategori pengamanan. Kategori pengamanan I yang terdiri atas 14 pertanyaan memperoleh nilai 7, kategori pengamanan II dengan 15 pertanyaan memperoleh nilai 8, sedangkan kategori pengamanan III yang terdiri atas 6 pertanyaan memperoleh nilai 9. Hasil tersebut menunjukkan bahwa penerapan teknologi keamanan informasi di Dinas Sosial GHI masih berada pada tahap awal dan belum dapat dikategorikan sebagai penerapan yang terdefinisi dan konsisten. Sebagian besar kontrol keamanan teknologi masih berstatus dalam perencanaan atau belum dilakukan, terutama pada aspek pencatatan dan analisis log, penerapan enkripsi, pengelolaan kata sandi dan akses administratif, perlindungan terhadap *malware*, pengembangan aplikasi yang aman (*secure coding*), pengamanan *source code*, serta pencegahan kebocoran data. Meskipun demikian, terdapat satu kontrol yang telah diterapkan secara menyeluruh, yaitu kaji ulang berkala terhadap konfigurasi keamanan perangkat komputasi serta pemantauan efektivitas dan pemutakhiran konfigurasinya melalui proses *change management*. Selain itu, beberapa kontrol seperti segmentasi jaringan, pemindaian kerentanan, pemantauan kapasitas, perlindungan akses dari luar, deteksi akses jaringan tidak resmi, perencanaan pengembangan sistem, dan validasi fungsi keamanan aplikasi masih berada dalam tahap perencanaan. Kondisi tersebut menunjukkan bahwa Dinas Sosial GHI perlu meningkatkan penerapan teknologi keamanan secara lebih menyeluruh, khususnya pada aspek pengendalian akses, pemantauan dan pencatatan aktivitas sistem, perlindungan data, keamanan jaringan, perlindungan terhadap malware, serta mekanisme deteksi dan penanganan insiden agar pengelolaan teknologi keamanan informasi semakin efektif dan selaras dengan SNI ISO/IEC 27001:2022 (Akbar, Gussati, et al., 2026; Marican et al., 2023; Zhang et al., 2021).

Perlindungan Data Pribadi Kategori

Kategori Perlindungan Data Pribadi (PDP) digunakan untuk mengevaluasi tingkat kelengkapan, konsistensi, dan efektivitas penerapan kontrol keamanan dalam

proses pengelolaan serta perlindungan data pribadi yang dimiliki organisasi (Akbar, Gussati, et al., 2026; Sun et al., 2022). Penilaian dilakukan berdasarkan empat status penerapan, yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh. Aspek PDP terdiri atas 16 butir pertanyaan yang digunakan untuk mengukur sejauh mana organisasi telah menerapkan kebijakan, prosedur, dan mekanisme dalam melindungi data pribadi. Dari keseluruhan pertanyaan tersebut, terdapat 4 butir pada kategori pengamanan I dan 12 butir pada kategori pengamanan II. Hasil evaluasi secara umum memberikan gambaran mengenai tingkat kesiapan organisasi dalam menerapkan kontrol perlindungan data pribadi sesuai dengan kebutuhan keamanan informasi. Meskipun beberapa mekanisme perlindungan telah diterapkan, peningkatan masih diperlukan terutama dalam memperkuat konsistensi penerapan pengendalian, penyempurnaan kebijakan dan prosedur, serta kepatuhan terhadap ketentuan perlindungan data pribadi yang berlaku. Rincian hasil evaluasi aspek Perlindungan Data Pribadi disajikan pada Tabel 8.

Tabel 8. Skor Evaluasi Perlindungan Data Pribadi

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	4	3
2	12	32
Total	**16**	**35**

Berdasarkan hasil evaluasi pada bagian PDP, diperoleh total skor sebesar 35 dari 16 butir pertanyaan yang terbagi ke dalam dua kategori pengamanan. Kategori pengamanan I terdiri atas 4 pertanyaan dengan nilai sebesar 3, sedangkan kategori pengamanan II terdiri atas 12 pertanyaan dengan nilai sebesar 32. Hasil tersebut menunjukkan bahwa penerapan perlindungan data pribadi pada Dinas Sosial GHI masih memerlukan peningkatan agar kebijakan, prosedur, dan mekanisme perlindungan data dapat diterapkan secara lebih menyeluruh dan konsisten. Meskipun beberapa kontrol perlindungan data pribadi telah diterapkan, masih terdapat aspek yang berada dalam tahap perencanaan maupun belum diterapkan sepenuhnya. Oleh karena itu, diperlukan penguatan pada aspek kebijakan, pengawasan, kepatuhan, pengelolaan hak pemilik data, serta peningkatan pemahaman pegawai mengenai pentingnya perlindungan data pribadi (Akbar, Veronica, et al., 2026; Chan et al., 2021). Upaya tersebut diperlukan untuk meningkatkan efektivitas pengelolaan dan perlindungan data pribadi serta mendukung penerapan keamanan informasi yang selaras dengan SNI ISO/IEC 27001:2022 dan ketentuan perlindungan data pribadi yang berlaku (Alkhazi et al., 2022).

Suplemen

Kategori suplemen merupakan bagian akhir dalam proses evaluasi yang digunakan untuk mengukur efektivitas pemanfaatan teknologi serta keterlibatan pihak ketiga dalam mendukung perlindungan aset informasi organisasi (Sugiarto & Suryanto, 2022). Penilaian pada kategori ini menggunakan empat status penerapan, yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh. Bagian ini mencakup satu kategori utama, yaitu pengamanan keterlibatan pihak ketiga, yang berfokus pada pengelolaan risiko, penerapan kebijakan keamanan, dan keberlangsungan layanan. Penilaian juga mencakup pengelolaan subkontraktor, perlindungan aset informasi, serta mekanisme penanganan

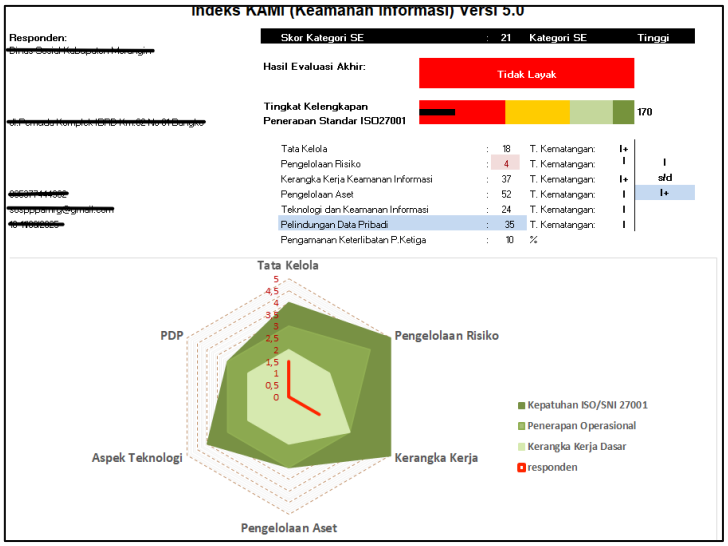
insiden yang berkaitan dengan pihak ketiga. Secara keseluruhan, kategori suplemen memberikan gambaran mengenai sejauh mana Dinas Sosial GHI telah mengintegrasikan kebijakan dan kontrol keamanan informasi dalam pelaksanaan kerja sama dengan pihak ketiga. Rincian hasil evaluasi pada kategori suplemen disajikan pada Tabel 9.

Tabel 9. Skor Evaluasi Suplemen

Kategori Pengamanan	Jumlah Pertanyaan	Nilai
1	27	0,30
Total	**27**	**10%**

Berdasarkan hasil evaluasi pada bagian suplemen, khususnya aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, terdapat 27 butir pertanyaan yang dievaluasi dengan total skor sebesar 8, nilai rata-rata sebesar 0,30, dan tingkat pencapaian sekitar 10%. Hasil tersebut menunjukkan bahwa penerapan pengamanan informasi terkait keterlibatan pihak ketiga pada Dinas Sosial GHI masih berada pada tahap awal dan belum dilaksanakan secara menyeluruh. Beberapa aspek telah mulai diterapkan atau berada dalam tahap perencanaan, terutama pada identifikasi risiko keamanan informasi dalam kerja sama dengan pihak ketiga, komunikasi dan mitigasi risiko, pengelolaan risiko subkontraktor, serta perencanaan pengelolaan dan pemantauan layanan pihak ketiga. Namun, sebagian besar kontrol masih berstatus tidak dilakukan, terutama yang berkaitan dengan penerapan kebijakan keamanan bagi pihak ketiga, hak audit, pemantauan kepatuhan subkontraktor, evaluasi SLA, audit keamanan pihak ketiga, pengelolaan perubahan layanan, penanganan dan pemusnahan aset, pengelolaan insiden, serta rencana kelangsungan layanan. Kondisi tersebut menunjukkan bahwa Dinas Sosial GHI masih perlu memperkuat tata kelola keamanan informasi dalam hubungan dengan pihak ketiga melalui penyusunan kebijakan dan prosedur yang terdokumentasi, peningkatan mekanisme pemantauan dan evaluasi, serta penerapan pengendalian risiko secara konsisten (Paramita et al., 2022). Oleh karena itu, diperlukan peningkatan secara bertahap dan berkelanjutan agar pengamanan keterlibatan pihak ketiga dapat semakin efektif dan mendukung tata kelola keamanan informasi yang selaras dengan prinsip SNI ISO/IEC 27001:2022 (Kawanishi et al., 2023).

Evaluasi kesiapan keamanan informasi pada Dinas Sosial GHI menggunakan Indeks KAMI versi 5.0 memberikan gambaran mengenai kondisi penerapan keamanan informasi pada berbagai area penilaian, meliputi tata kelola, pengelolaan risiko, kerangka kerja keamanan informasi, pengelolaan aset, teknologi keamanan, pelindungan data pribadi, serta pengamanan keterlibatan pihak ketiga. Hasil evaluasi tersebut menunjukkan tingkat kesiapan dan kematangan yang berbeda pada setiap area, sehingga dapat digunakan untuk mengidentifikasi aspek yang telah diterapkan maupun bagian yang masih memerlukan peningkatan. Secara keseluruhan, hasil penilaian menjadi dasar bagi Dinas Sosial GHI dalam menyusun prioritas dan strategi peningkatan keamanan informasi secara bertahap agar semakin selaras dengan SNI ISO/IEC 27001:2022 (Akbar, Veronica, et al., 2026). Gambar 2 menyajikan hasil evaluasi tingkat kematangan keamanan informasi berdasarkan masing-masing area penilaian yang telah diukur.



Gambar 2. Dashboard Penilaian Indeks KAMI 5 Hasil

Hasil evaluasi akhir menggunakan Indeks KAMI Versi 5.0 menunjukkan bahwa Dinas Sosial GHI memperoleh skor 21 pada Kategori Sistem Elektronik (SE) dan termasuk dalam kategori Tinggi. Sementara itu, tingkat kelengkapan penerapan standar ISO/IEC 27001 memperoleh skor sebesar 170, sehingga hasil evaluasi akhir berada pada kategori "Tidak Layak". Berdasarkan Gambar 2, nilai masing-masing area penilaian menunjukkan bahwa Tata Kelola memperoleh skor 18 dengan tingkat kematangan I+, Pengelolaan Risiko memperoleh skor 4 dengan tingkat kematangan I, Kerangka Kerja Keamanan Informasi memperoleh skor 37 dengan tingkat kematangan I+, Pengelolaan Aset memperoleh skor 52 dengan tingkat kematangan I, Teknologi dan Keamanan Informasi memperoleh skor 24 dengan tingkat kematangan I, serta Pelindungan Data Pribadi memperoleh skor 35 dengan tingkat kematangan I. Selain itu, aspek Pengamanan Keterlibatan Pihak Ketiga memperoleh tingkat pencapaian sebesar 10%. Hasil tersebut menunjukkan bahwa meskipun kategori Sistem Elektronik Dinas Sosial GHI tergolong tinggi, tingkat kelengkapan dan kematangan penerapan keamanan informasi masih relatif rendah dan belum memenuhi tingkat kesiapan yang dipersyaratkan. Oleh karena itu, diperlukan peningkatan secara menyeluruh, khususnya pada pengelolaan risiko, pengamanan teknologi, pengelolaan aset, pelindungan data pribadi, serta pengamanan keterlibatan pihak ketiga agar penerapan keamanan informasi dapat berkembang menuju tingkat yang lebih terstruktur, konsisten, dan sesuai dengan SNI ISO/IEC 27001:2022 (Akbar, Veronica, et al., 2026; Habibullah et al., 2024; Imtikhan Azmi et al., 2024).

Berdasarkan hasil evaluasi pada Dinas Sosial GHI, dilakukan perbandingan hasil penilaian Indeks KAMI dengan beberapa instansi lain yang telah menjadi objek penelitian sebelumnya. Perbandingan ini bertujuan untuk melihat posisi relatif tingkat kesiapan dan kematangan keamanan informasi Dinas Sosial GHI dibandingkan dengan organisasi sejenis. Melalui perbandingan tersebut, dapat diidentifikasi kesenjangan maupun aspek yang memerlukan peningkatan dalam penerapan keamanan informasi. Hasil perbandingan selengkapnya disajikan pada Tabel 10.

Tabel 10. Perbandingan Hasil Evaluasi

Institusi	Versi Indeks KAMI	Skor Total	Tingkat Kematangan	Kategori
Dinas Sosial GHI	5.0	170	I-I+	Tidak Layak
BAWASLU ABC	5.0	918	III-V	Baik
Pengadilan Negeri BKO	5.0	913	III-V	Baik
SMK XYZ	4.2	314	I-II	Tidak Layak

Berdasarkan hasil perbandingan tingkat kesiapan keamanan informasi menggunakan Indeks KAMI, dapat disimpulkan bahwa Dinas Sosial GHI memiliki tingkat kesiapan keamanan informasi yang masih relatif rendah dibandingkan dengan beberapa institusi lain pada Tabel 10. Dinas Sosial GHI memperoleh skor total 170 dengan tingkat kematangan I–I+ dan termasuk dalam kategori "Tidak Layak". Nilai tersebut lebih rendah dibandingkan BAWASLU ABC yang memperoleh skor 918 dengan tingkat kematangan III–V dan kategori "Baik", serta Pengadilan Negeri BKO dengan skor 913 pada tingkat kematangan III–V dan kategori "Baik". Dibandingkan dengan SMK XYZ, Dinas Sosial GHI juga memiliki skor yang lebih rendah, meskipun penilaian SMK XYZ menggunakan Indeks KAMI versi 4.2, sehingga perbandingan skor secara langsung perlu dilakukan secara hati-hati. Secara keseluruhan, hasil ini menunjukkan bahwa Dinas Sosial GHI masih memerlukan peningkatan yang signifikan pada berbagai aspek keamanan informasi agar tingkat kematangan dan kesiapan penerapan keamanan informasi dapat meningkat menuju kategori yang lebih baik.

KESIMPULAN

Berdasarkan hasil analisis dan evaluasi keamanan informasi menggunakan Indeks KAMI Versi 5.0, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Hasil evaluasi menunjukkan bahwa Dinas Sosial GHI memperoleh skor 21 pada Kategori Sistem Elektronik (SE) sehingga termasuk dalam kategori Tinggi. Sementara itu, tingkat kelengkapan penerapan standar keamanan informasi memperoleh skor total 170 dengan hasil evaluasi akhir "Tidak Layak" dan tingkat kematangan berada pada rentang I–I+. Kondisi tersebut menunjukkan bahwa meskipun sistem elektronik yang dikelola memiliki tingkat kepentingan yang tinggi, kesiapan penerapan keamanan informasi Dinas Sosial GHI masih belum memadai. Oleh karena itu, diperlukan peningkatan secara bertahap dan berkelanjutan pada kebijakan, prosedur, pengelolaan risiko, pengamanan aset dan teknologi, pelindungan data pribadi, serta pengelolaan keamanan pihak ketiga agar penerapan keamanan informasi semakin selaras dengan SNI ISO/IEC 27001:2022.
2. Berdasarkan hasil evaluasi pada masing-masing area, Tata Kelola Keamanan Informasi memperoleh skor 18 dengan tingkat kematangan I+, Pengelolaan Risiko sebesar 4 dengan tingkat kematangan I, Kerangka Kerja Pengelolaan Keamanan Informasi sebesar 37 dengan tingkat kematangan I+, Pengelolaan Aset Informasi sebesar 52 dengan tingkat kematangan I, Teknologi dan Keamanan Informasi sebesar 24 dengan tingkat kematangan I, serta Pelindungan Data Pribadi sebesar 35

dengan tingkat kematangan I. Sementara itu, Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan memperoleh tingkat pencapaian sebesar 10%. Hasil tersebut memperlihatkan bahwa sebagian besar area keamanan informasi masih berada pada tahap awal penerapan, dengan sejumlah kontrol masih dalam perencanaan maupun belum dilaksanakan. Dengan demikian, prioritas peningkatan perlu diarahkan terutama pada pengelolaan risiko, teknologi keamanan, pelindungan data pribadi, serta pengamanan keterlibatan pihak ketiga.

3. Penelitian ini menggunakan Indeks KAMI Versi 5.0 untuk mengevaluasi kesiapan keamanan informasi pada Dinas Sosial GHI, sehingga memberikan gambaran aktual mengenai kondisi keamanan informasi pada instansi pemerintah yang mengelola berbagai data dan layanan sosial. Berdasarkan perbandingan dengan penelitian sebelumnya, Dinas Sosial GHI memperoleh skor 170 dengan tingkat kematangan I–I+ dan kategori "Tidak Layak", lebih rendah dibandingkan BAWASLU ABC dengan skor 918 dan Pengadilan Negeri BKO dengan skor 913 yang masing-masing berada pada tingkat kematangan III–V dengan kategori "Baik". Dinas Sosial GHI juga memperoleh skor lebih rendah dibandingkan SMK XYZ yang memperoleh skor 314 dengan tingkat kematangan I–II dan kategori "Tidak Layak"; namun, perbandingan tersebut perlu dilakukan secara hati-hati karena SMK XYZ menggunakan Indeks KAMI Versi 4.2. Hasil penelitian ini menunjukkan bahwa Indeks KAMI Versi 5.0 dapat digunakan sebagai instrumen evaluasi untuk mengidentifikasi kesenjangan, menentukan prioritas perbaikan, serta menjadi dasar penyusunan kebijakan dan strategi peningkatan keamanan informasi yang lebih terarah dan berkelanjutan dalam menghadapi perkembangan risiko dan ancaman siber.

DAFTAR PUSTAKA

Akbar, M. T., Gussati, R., Pradiva, M. A. R., Refina, Ferlica, E. Y., Afriandi, T. M., Lestari, D. A. I., & Husadi, H. (2026). *An Information Security Maturity Evaluation of the BKO District Court Based on the KAMI Index Version 5.0*. *15*(2), 65–75. https://doi.org/https://doi.org/10.18495/comengapp.v15i2.1329

Akbar, M. T., & Siregar, M. U. (2024). *A Survey on Software Requirements Engineering in Information Technology Institutions*. *9*(2), 253–264. https://doi.org/https://doi.org/10.21831/elinvo.v9i2.70862

Akbar, M. T., Veronica, R. T., Widyana, R. I., & Nurahman, H. (2026). *Evaluasi Kesiapan Keamanan Informasi BAWASLU ABC Menggunakan Indeks KAMI 5.0*. *9*(1), 88–97. https://doi.org/https://doi.org/10.14421/csecurity.2026.9.1.5709

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

Bagaskara, B. A., Idhom, M., & Wahanani, H. E. (2025). *PENGUJIAN WEBSITE DINAS SOSIAL SURABAYA MENGGUNAKAN METODE PENETRATION TESTING DAN OWASP TOP 10*. *8*(1), 40–50.

Bakhtiar, A., & Salsabila Hidayat, F. (2023). EVALUASI SISTEM MANAJEMEN

KEAMANAN INFORMASI BERDASARKAN PENILAIAN INDEKS KAMI v.4.2 PADA DINAS XYZ PROVINSI JAWA TENGAH. *Industrial Engineering Online Journal*, *12*(4). https://ejournal3.undip.ac.id/index.php/ieoj/article/view/41401

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

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

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

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

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

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

Karunia, W. A., Zahra, A. F., & 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), 10–16.

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

Khusna, T. N., & 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), 847–856. https://doi.org/10.29100/jipi.v8i3.3720

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

Paramita, S., Siregar, S. A., Damanik, R. A., & ... (2022). Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013. *Bulletin of Information ...*, *3*(4), 374–379. 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), 181–187.

Sugiarto, P., & 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), 974–5823.

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

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