Jurnal Publikasi Manajemen Informatika
Volume 5 Nomor 1 Januari 2026
E-ISSN : 2808-9014; P-ISSN 2808-9359, Hal 112-123
DOI: https://doi.org/10.55606/jupumi.v5i1.4473
Tersedia: https://journalcenter.org/index.php/jupumi

SISTEM MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN ISO 27001 PADA SISTEM INFORMASI PENELUSURAN PERKARA (SIPP)

Gilang Derman Dida[1*], Menhya Snae[2]

[1]Sistem Informasi Strata Satu, STIKOM Uyelindo Kupang, Indonesia
gilangdida2@gmail.com
[2]Sistem Informasi Strata Satu, STIKOM Uyelindo Kupang, Indonesia

Alamat: Jl. Perintis Kemerdekaan 1, Kelurahan Kayu Putih, Kota Kupang, Nusa Tenggara Timur
Korespondensi penulis: gilangdida2@gmail.com

Abstract. *With the advancement of technology that continues to grow, its influence on various aspects of education, including government, is increasingly felt. One example is the Military Court III-15 Kupang, as an agency engaged in law enforcement, therefore, it is important to have an effective information security management system in accordance with the ISO 27001 security standard. However, the problem faced by Military Court III-15 Kupang is information security. Information security is an important thing to be considered by information technology management and it is necessary to measure the strength of information security. This research aims to develop recommendations for improving the Information Security System to strengthen the information security management system at the Military Court Office III-15 Kupang, while the method used is measurement with the Information Security index (KAMI). To determine the level of information security in the Case Tracking Information System (SIPP) at Military Court III-15 Kupang. The expected result is the creation of a structured, systematic and reliable information security management system to support military court operations that are safe, efficient and in accordance with ISO 27001 standards.*

Keywords: *ISO 27001, Information System, Information Security, Security Management, Security System.*

Abstrak. Kemajuan teknologi yang terus berkembang, pengaruhnya terhadap berbagai aspek pendidikan, termasuk pemerintahan, semakin terasa. Salah satu contohnya adalah Pengadilan Militer III-15 Kupang, sebagai instansi yang bergerak dalam bidang penegakan hukum oleh karna itu, penting untuk memiliki sistem manajemen keamanan informasi yang efektif sesuai dengan standar keamanan ISO 27001. Namuna masalah yang dihadapi Pengadilan Militer III-15 Kupang adalah keamanan informasi. Keamanan informasi merupakan hal yang penting untuk diperhatikan oleh pihak manajemen teknologi informasi dan perlu dilakukan pengukuran terhadap kekuatan dari keamanan informasi. Penelitian ini bertujuan untuk Menyusun Rekomendasi Peningkatan Sistem Keamanan Informasi untuk memperkuat sistem manajemen keamanan informasi di Kantor Pengadilan Militer III-15 Kupang, adapun metode yang digunkana adalah pengukuran dengan indeks Keamanan Informasi (KAMI). Untuk mengetahui tingkat keamanan informasi pada Sistem Informasi Penelusuran Perkara (SIPP) di Pengadilan Militer III-15 Kupang. Hasil yang diharapkan adalah terciptanya sistem manajemen keamanan informasi yang terstruktur, sistematis dan dapat diandalkan untuk mendukung oprasional pengadilan militer yang aman, efisien dan sesuai dengan standar ISO 27001.

Kata kunci: ISO 27001, Keamanan Informasi, Manajemen Keamanan, Sistem Informasi, Sistem Keamanan.

1. LATAR BELAKANG

Teknologi informasi merupakan sumber daya strategis, yang dapat menyediakan informasi penting untuk membantu dalam pengambilan keputusan pada sebuah organisasi . Salah satu bagian yang mempengaruhi teknologi informasi adalah keamanan informasi.

Naskah Masuk: 14 Juni 2025; Revisi: 12 Juli 2025; Diterima: 11 November 2025; Tersedia: 15 Desember 2025; Terbit: 05 Januari 2026;

Keamanan informasi merupakan hal yang penting untuk diperhatikan oleh pihak manajemen teknologi informasi dan perlu dilakukan pengukuran terhadap kekuatan dari keamanan informasi yang telah diterapkan. Kekuatan keamanan informasi dapat dikontrol menggunakan sistem manajemen keamanan informasi, berfungsi untuk mengatur dan mengoperasikan keamanan sistem informasi agar dapat digunakan sesuai dengan prosedur. Tujuan dari sistem manajemen keamanan informasi adalah menjamin kerahasiaan, keutuhan, dan ketersediaan dari data dan informasi (Octariza, 2019).

ISO 27001 adalah standar internasional yang menyediakan kerangka kerja dan panduan untuk mengelola risiko keamanan informasi dalam sebuah organisasi. Standar ini juga dikenal sebagai Sistem Manajemen Keamanan Informasi (SMKI). Dirilis oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC). Tujuan utamanya adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi melalui penerapan proses manajemen risiko dan memberikan kepercayaan kepada para pemangku kepentingan. SMKI yang sesuai dengan ISO/IEC 27001 mencakup kebijakan keamanan informasi, manajemen risiko, kontrol keamanan, manajemen akses, dan pemantauan kinerja keamanan informasi.

Berdasarkan hasil wawancara yang dilakukan oleh peneliti terhadap Kepala Bagian Perencanaan, Informasi Teknologi dan Pelaporan, dijelaskan bahwa Sistem Informasi Penelusuran Perkara (SIPP) pada Pengadilan Militer III-15 Kupang memiliki beberapa data sensitif yang tidak boleh diketahui oleh banyak oramg seperti perkara asusila yang nama pelakunya disamarkan sehingga hanya admin yang bisa melihat secara riil. Oleh karena Itu, telah dijelaskan sebelumnya bahwa informasi merupakan aset yang sangat berharga dan jika pengelolaan terhadap aset ini baik maka akan menjadikan kemampuan manajerial dan pelayanan Pengadilan Militer III-15 Kupang terhadap publik semakin baik.

Merujuk pada peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016, tentang sistem manajemen pengamanan informasi tertulis bahwa setiap penyelenggara sistem elektronik harus melakukankeamanan terhadap informasi dalam kepentingan umum, pelayanan publik, kelancaran penyelenggaraan Negara, atau pertahanan dan keamanan Negara, dari peraturan ini diketahui dengan jelas bahwa sangat diperlukannya sebuah keamanan informasi yang dapatmemenuhi peraturan Menteri Komunikasi dan Informatika Republik Indonesia tersebut.

2. KAJIAN TEORITIS

Menurut Sarno dan Iffano menerapkan teknik keamanan saja maka akan menjamin 100% aman. Walaupun teknik-teknik keamanan tersebut terhimpun dalam Teknologi Keamanan Informasi, belum cukup untuk memberikan jaminan keamanan yang menyeluruh. Hal lain yang diperlukan adalah sistem yang mengelola Teknologi Informasi dalam proses-proses sekaligus penjagaan terhadap aspek Keamanan Informasi yang disebut dengan SMKI. Kedua hal tersebut merupakan elemen penting dalam Keamanan Informasi (Chazar, 2015).

Menurut Sarno (2009), standar ISO/IEC 27001:2013 adalah suatu standar sistem manajemen keamanan informasi yang memberikan panduan secara umum mengenai prosedur perusahaan yang harus dilakukan dalam proses evaluasi, implementasi, dan pengendalian keamanan informasi berdasarkan praktik terbaik dalam pengendalian perlindungan informasi (Nurfadilah, et.al., 2020).

Matriks penilaian berfungsi sebagai acuan dalam memberikan penilaian pada saat Perhitungan Data dan penentuan status Tingkat Kesiapan. Adapun matriks penilaian yang digunakan adalah sebagai berikut (Khamil, et.al., 2022).

Setiap klausul dalam ISO 27001 memiliki persyaratan yang diharuskan terpenuhi oleh organisasi untuk memastikan perlindungan informasi yang efektif. Organisasi harus mengevaluasi dan mengelola risiko keamanan informasi, mengimplementasikan kontrol keamanan yang sesuai, dan secara terus-menerus meningkatkan sistem manajemen keamanan informasi mereka untuk memenuhi persyaratan standar (Rutanaji, et.al., 2018). Dari 14 Klausul diatas peneliti menggunakan, Klausul 2 Organisasi keamanan informasi pada ISO 27001 dikarenakan di klausul tersebut menjelaskan tentang proses *risk assessment*. Klausul ini menjelaskan bahwa organisasi harus mengevaluasi risiko keamanan informasi yang mungkin timbul dan mengambil tindakan yang sesuai untuk mengelola dan mengurangi risiko tersebut. Klausul ini juga menjelaskan bahwa organisasi harus mengevaluasi risiko secara berkala dan melakukan tindakan yang sesuai digunakan mengatasi risiko yang muncul dari perubahan lingkungan operasional atau perubahan dalam sistem, aplikasi atau data.

3. METODE PENELITIAN

Penelitian ini diawali dengan tahap identifikasi masalah yang dilakukan melalui pengamatan langsung di lingkungan Pengadilan Militer III-15 Kupang. Hasil observasi menunjukkan bahwa belum pernah dilakukan pengukuran terhadap keamanan informasi,

khususnya pada Sistem Informasi Penelusuran Perkara (SIPP), sehingga tingkat kelengkapan dan kematangan sistem keamanan informasi belum diketahui secara pasti. Untuk mendukung pemahaman teori dan landasan metodologis, dilakukan studi literatur dengan mengkaji referensi-referensi yang relevan, termasuk standar ISO 27001 dan pedoman Indeks KAMI.

Data penelitian dikumpulkan melalui tiga metode utama, yaitu observasi lapangan, wawancara kepada Kepala Bagian Perencanaan, Teknologi Informasi dan Pelaporan (PTIP), serta penyebaran kuesioner kepada seluruh staf PTIP. Kuesioner disusun berdasarkan indikator dalam Indeks KAMI untuk memperoleh gambaran menyeluruh mengenai kondisi keamanan informasi pada SIPP. Setelah data terkumpul, dilakukan proses tabulasi untuk menyusun data ke dalam bentuk tabel agar lebih mudah dianalisis.

Tahap berikutnya adalah perhitungan menggunakan metode Indeks KAMI, yang bertujuan untuk mengetahui sejauh mana tingkat kematangan dan kelengkapan pengelolaan keamanan informasi di instansi tersebut. Hasil perhitungan ini menjadi dasar dalam merumuskan rekomendasi perbaikan. Rekomendasi disusun dengan mengacu pada standar ISO 27001 dan disesuaikan dengan kondisi organisasi, sehingga dapat dijalankan secara bertahap untuk meningkatkan sistem keamanan informasi yang ada secara berkelanjutan.

4. HASIL DAN PEMBAHASAN

1. Matriks Penilaian

Setiap pertanyaan di masing-masing area akan masuk kedalam 3 Kategori Pengamanan (KP). Semakin tinggi kategori pengamanan dan semakin tinggi status penerapannya maka akan semakin besar skor yang didapatkan. Adapun matriks yang digunakan dapat dilihat pada Tabel 1 sebagai berikut (Khamil, et.al., 2022).

Tabel 1. Matriks kategori pengamanan

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

Status Tingkat Kesiapan didapatkan berdasarkan korelasi antara skor akhir Kategori Sistem Elektronik dan skor akhir Kategori Keamanan Informasi. Adapun matriks yang

digunakan dapat dilihat pada Tabel 2 sebagai berikut (Khamil, et.al., 2022).

Tabel 2. Matriks skor akhir dan status tingkat kesiapan

Kategori Sistem Elektronik		**Kategori Keamanan Informasi**		**Status Kesiapan**
Rendah		**Skor Akhir**		
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

2. Analisis KAMI

Indeks KAMI (Keamanan Informasi) merupakan salah satu indikator yang digunakan untuk mengukur stabilitas sosial dan potensi gangguan keamanan di wilayah kerja Pengadilan Militer III-15 Kupang. Dalam konteks Sistem Informasi Penelusuran Perkara (SIPP), Indeks KAMI digunakan untuk mengidentifikasi hubungan antara beban perkara, jenis pelanggaran, dan kecenderungan situasi sosial di masyarakat militer yang menjadi yurisdiksi pengadilan. Nilai indeks ini disusun berdasarkan sejumlah variabel, seperti jumlah perkara yang masuk, jenis perkara dominan, tingkat penyelesaian perkara, serta tingkat keterlibatan elemen masyarakat atau militer dalam kasus-kasus tertentu. Data yang diolah menunjukkan kecenderungan tertentu yang dapat digunakan sebagai bahan evaluasi keamanan institusi, efektivitas sistem penelusuran perkara, dan kesiapsiagaan lembaga dalam menjaga stabilitas internal maupun eksternal. Dengan memasukkan data real-time dari SIPP ke dalam pengukuran Indeks KAMI, diharapkan dapat diperoleh gambaran yang lebih akurat dan responsif terhadap potensi ancaman atau gangguan keamanan di lingkungan peradilan militer.

a) Kategori sistem elektronik

Berdasarkan hasil penilaian terhadap sepuluh karakteristik utama yang mencerminkan kompleksitas, risiko, dan dampak dari sistem elektronik yang dikelola, sistem ini dikategorikan sebagai Sistem Elektronik dengan Tingkat Ketergantungan Tinggi dengan

total skor sebesar 26. Rincian Penilaian yaitu nilai investasi sistem elektronik *(Skor: 1),* anggaran operasional tahunan *(Skor: 1),* Kepatuhan terhadap regulasi/standar *(Skor: 2),* penggunaan teknik kriptografi *(Skor: 2),* jumlah pengguna *(Skor: 5),* jenis data pribadi yang dikelola *(Skor: 5),* klasifikasi/kekritisan data *(Skor: 5),* kekritisan proses dalam sistem *(Skor: 2),* dampak kegagalan sistem *(Skor: 2),* dan potensi kerugian dari insiden keamanan *(Skor: 2)*.

Dengan total skor 26, sistem ini dikategorikan sebagai Sistem Elektronik dengan Tingkat Ketergantungan Tinggi, menandakan bahwa sistem memiliki pengaruh besar terhadap publik, memproses data yang sangat sensitif, dan memiliki basis pengguna yang luas. Oleh karena itu, sistem ini memerlukan pengelolaan keamanan informasi yang kuat, kepatuhan regulasi yang ketat, serta pengawasan yang berkelanjutan untuk memastikan keandalan dan integritas operasionalnya.

b) Tata kelola keamanan informasi

Penilaian terhadap aspek Tata Kelola Keamanan Informasi menunjukkan bahwa instansi/perusahaan telah memiliki struktur, tanggung jawab, dan praktik pengelolaan keamanan informasi yang cukup matang dan terintegrasi, dengan total skor sebesar 67, yang menempatkan sistem dalam kategori Tingkat Ketergantungan Tinggi.

Rincian temuan utama:

1. Komitmen pimpinan dan kebijakan

   Pimpinan instansi secara resmi bertanggung jawab terhadap pelaksanaan program keamanan informasi dan penetapan kebijakan terkait. *(Skor: 3)*

   Peran keamanan informasi telah melekat dalam proses kerja dan koordinasi lintas fungsi internal maupun eksternal dilakukan secara proaktif. *(Skor: 6)*
2. Struktur organisasi dan fungsi pengelola keamanan

   Terdapat fungsi atau unit khusus yang mengelola keamanan informasi, dengan personel yang memiliki wewenang memadai. *(Skor: 3 masing-masing)*

   Penanggung jawab telah diberikan sebagian sumber daya dan peran-peran pelaksana mulai dipetakan dengan baik. *(Skor: 2 masing-masing)*
3. Kompetensi dan sumber daya manusia

   Persyaratan kompetensi telah didefinisikan dan ada upaya peningkatan kapasitas melalui pelatihan berkelanjutan. *(Skor: 3 dan 6)*

Namun, pelaksanaan kompetensi secara menyeluruh masih dalam tahap penerapan sebagian. *(Skor: 2)*

4. Kesadaran dan sosialisasi

   Program sosialisasi keamanan informasi sudah berjalan menyeluruh, memperkuat pemahaman dan kepatuhan internal. *(Skor: 3)*

5. Integrasi dan pemantauan dalam proses kerja

   Keamanan informasi telah diintegrasikan dalam proses kerja, termasuk pengamanan data pribadi, pelaporan berkala, dan kesinambungan layanan (business continuity). *(Skor: 6 untuk tiap poin terkait)*

6. Keterlibatan strategis dan koordinasi eksternal

   Keamanan informasi telah menjadi bagian dari pertimbangan strategis pimpinan dan diterapkan oleh satuan kerja terkait. *(Skor: 6)*

7. Kekurangan

   Meskipun banyak area telah diterapkan dengan baik, terdapat beberapa aspek penting yang belum mendapatkan skor (Skor: 0), seperti:

   a. Pemetaan dan evaluasi sasaran kinerja pengelolaan keamanan informasi.
   b. Penerapan metrik dan indikator kinerja keamanan informasi.
   c. Penilaian kinerja individu pelaksana keamanan informasi.
   d. Identifikasi dan analisis kepatuhan terhadap peraturan/perundangan.
   e. Kebijakan khusus penanggulangan insiden hukum.

Dengan total skor 67, tata kelola keamanan informasi berada dalam kategori Tingkat Ketergantungan Tinggi, menunjukkan bahwa sistem ini sangat bergantung pada efektivitas pengelolaan keamanan informasi. Mayoritas elemen fundamental telah diterapkan secara menyeluruh, namun terdapat ruang perbaikan di area pengukuran, pelaporan kinerja, dan manajemen risiko hukum.

c) Pengelolaan resiko keamanan informasi

Berdasarkan hasil penilaian KAMI (Keamanan Informasi) pada aspek Pengelolaan Risiko Keamanan Informasi, dapat disimpulkan bahwa instansi telah menerapkan seluruh komponen pengelolaan risiko secara menyeluruh dan terdokumentasi dengan baik. Program kerja pengelolaan risiko keamanan informasi sudah tersedia dan digunakan secara resmi, serta telah ditetapkan penanggung jawab manajemen risiko yang dapat melakukan eskalasi pelaporan hingga ke tingkat pimpinan. Kerangka kerja pengelolaan risiko yang diterapkan

mencakup seluruh aspek penting, seperti klasifikasi aset informasi, identifikasi ancaman dan kelemahan, serta penetapan dampak kerugian terhadap aset utama. Selain itu, instansi juga telah menentukan ambang batas risiko yang dapat diterima serta menetapkan kepemilikan dan pengelolaan aset secara jelas. Proses identifikasi, analisis, dan evaluasi risiko dilakukan secara terstruktur, dilengkapi dengan langkah mitigasi yang disusun berdasarkan prioritas, target waktu penyelesaian, dan efektivitas penggunaan sumber daya.

d) Kerangka kerja pengelolaan keamanan informasi

Berdasarkan hasil penilaian KAMI (Keamanan Informasi) pada aspek *Kerangka Kerja Pengelolaan Keamanan Informasi*, instansi menunjukkan penerapan yang menyeluruh dan sistematis terhadap seluruh kebijakan, prosedur, strategi, serta program keamanan informasi. Seluruh kebijakan dan prosedur yang dibutuhkan telah disusun secara jelas, mencakup peran serta tanggung jawab setiap pihak terkait, dan dikomunikasikan secara efektif kepada seluruh pegawai maupun pihak ketiga. Dokumen kebijakan dikelola dengan mekanisme resmi, termasuk distribusi dan penyimpanannya, serta tersedia proses untuk menindaklanjuti perubahan kebijakan, insiden keamanan, maupun kondisi yang memerlukan pengecualian.

Secara keseluruhan, kerangka kerja pengelolaan keamanan informasi instansi telah mencerminkan tingkat kematangan yang tinggi, dengan integrasi menyeluruh ke dalam tata kelola organisasi, proses bisnis, serta pengembangan teknologi yang aman dan berkelanjutan. Hal ini tercermin dari total skor penilaian yang diperoleh, yaitu 192, yang menunjukkan bahwa seluruh komponen telah diterapkan secara menyeluruh dan konsisten.

e) Pengelolaan aset informasi

Berdasarkan hasil penilaian pada aspek Pengelolaan Aset Informasi, instansi telah menunjukkan kemajuan yang baik dalam pendataan, klasifikasi, dan pengamanan aset informasi. Sebagian besar kontrol dasar, seperti penyusunan inventaris aset informasi, klasifikasi berdasarkan tingkat kepentingan dan regulasi, serta pengelolaan perubahan dan konfigurasi sistem, telah diterapkan secara menyeluruh. Prosedur-prosedur penting, seperti pemantauan back-up data, pengamanan infrastruktur komputasi, hingga pengamanan layanan berbasis cloud juga telah dijalankan dengan sistematis. Selain itu, beberapa kebijakan seperti pelaporan insiden, pengamanan fisik ruang kerja, dan pengelolaan akses juga sudah tersedia dan diterapkan.

Secara keseluruhan, penerapan pengelolaan aset informasi telah dilakukan dengan cukup baik dan mencerminkan adanya sistem tata kelola yang terstruktur. Hal ini tercermin dari total skor yang diperoleh sebesar 168, yang menunjukkan bahwa sebagian besar kontrol telah tersedia, meskipun masih ada ruang perbaikan pada sejumlah aspek penting untuk mencapai kepatuhan dan keamanan informasi yang optimal.

f) Teknologi dan keamanan informasi

Dalam aspek Teknologi dan Keamanan Informasi, instansi telah menunjukkan komitmen tinggi terhadap penerapan kontrol keamanan secara menyeluruh pada berbagai komponen infrastruktur dan sistem informasi. Sebagian besar pengamanan dasar hingga lanjutan telah diterapkan secara menyeluruh, seperti pemindaian kelemahan sistem secara berkala, pemantauan kapasitas dan efektivitas keamanan, penggunaan antivirus yang diperbarui secara rutin, pengamanan terhadap akses jaringan tidak resmi, serta penerapan prinsip pengembangan aplikasi yang aman (*secure coding*) dan pengujian kode sebelum produksi. Kontrol lanjutan seperti penerapan DLP (*Data Leakage Prevention*), pengamanan lingkungan pengembangan, dan mitigasi terhadap ancaman baru juga sudah dijalankan dengan baik.

Secara keseluruhan, kondisi ini mencerminkan bahwa instansi telah memiliki sistem keamanan informasi berbasis teknologi yang kuat, dengan sebagian besar komponen pengamanan telah tersedia dan berfungsi sesuai standar industri. Namun, untuk mencapai tingkat maturitas yang optimal, perlu dilakukan penguatan pada aspek pengamanan akses, manajemen enkripsi, dan keterlibatan pihak independen untuk penilaian eksternal secara berkala.

g) Pelindungan data pribadi

Dalam aspek Pelindungan Data Pribadi, instansi telah menunjukkan komitmen dan kepatuhan yang sangat baik terhadap peraturan dan prinsip perlindungan data sebagaimana diatur dalam perundang-undangan yang berlaku. Seluruh kontrol yang dinilai telah diterapkan secara menyeluruh, mencakup pendokumentasian data pribadi yang dikelola, pemetaan alur pemrosesan data, hingga penerapan kebijakan formal yang relevan. Selain itu, instansi juga telah menetapkan unit atau pejabat yang bertanggung jawab atas pelindungan data pribadi, melakukan kajian risiko terkait data pribadi, dan menerapkan mekanisme mitigasi sesuai dengan hasil analisis risiko serta ketentuan hukum.

Tidak hanya dari sisi teknis dan prosedural, instansi juga telah membangun kesadaran internal melalui program peningkatan pemahaman bagi seluruh pegawai, serta menjamin hak-hak pemilik data seperti akses, koreksi, dan penghapusan data. Proses-proses penting seperti permintaan persetujuan data pribadi, pelaporan insiden kebocoran, serta prosedur pengungkapan kepada aparat penegak hukum juga telah diterapkan dengan baik. Dengan total skor 84, ini mencerminkan bahwa pelindungan data pribadi di instansi tersebut sudah berada pada tingkat maturitas yang tinggi, sehingga mendukung penerapan keamanan informasi yang holistik dalam kerangka KAMI (Keamanan Informasi).

h) Pengamanan keterlibatan pihak ketiga penyedia layanan

Dalam aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, instansi telah menerapkan sebagian besar kontrol keamanan informasi secara menyeluruh, mencerminkan tingkat kepatuhan yang tinggi terhadap tata kelola hubungan dengan pihak ketiga. Mulai dari penetapan kebijakan, komunikasi risiko, hingga penyusunan kontrak yang mencakup persyaratan keamanan seperti pengendalian akses, penghapusan data, dan hak audit, sebagian besar poin telah diterapkan sepenuhnya. Prosedur formal dalam menangani data dan aset informasi sepanjang siklus hidupnya juga telah dijalankan dengan baik oleh pihak ketiga, termasuk prosedur penghancuran data secara aman.

Meski begitu, masih terdapat beberapa area yang belum sepenuhnya optimal, seperti identifikasi awal risiko keamanan dalam kerja sama dengan pihak ketiga, pelaporan SLA dan penalti, serta pengelolaan perubahan layanan dan kebijakan yang masih dalam tahap penerapan sebagian. Selain itu, keberadaan tim khusus dalam penanganan kelangsungan layanan pihak ketiga juga masih dalam proses penerapan.

Dengan total nilai evaluasi sebesar 88%, dapat disimpulkan bahwa instansi telah memiliki kapasitas pengamanan yang kuat dalam mengelola hubungan kerja sama dengan pihak ketiga, meskipun tetap perlu peningkatan dalam aspek identifikasi risiko awal, dokumentasi SLA, dan pemantauan kinerja pihak ketiga secara menyeluruh. Hal ini penting untuk memastikan bahwa semua mitra eksternal tetap menjaga standar keamanan informasi yang sejalan dengan kebijakan instansi.

3. Analisis ISO 27001

Dalam upaya meningkatkan kualitas tata kelola teknologi informasi, penerapan ISO 27001 dan KAMI (Keamanan Informasi) memiliki korelasi yang signifikan terhadap

pengelolaan Sistem Informasi Penelusuran Perkara (SIPP) di Pengadilan Militer III-15 Kupang. ISO 27001 merupakan standar internasional dalam sistem manajemen keamanan informasi (Information Security Management System/ISMS) yang bertujuan untuk melindungi kerahasiaan, integritas, dan ketersediaan data. Sementara itu, KAMI merupakan Kerangka Kerja Keamanan Informasi yang disusun oleh Badan Siber dan Sandi Negara (BSSN) sebagai panduan untuk mengukur dan meningkatkan tingkat kematangan keamanan informasi di instansi pemerintah. Dalam konteks SIPP yang berfungsi sebagai sistem elektronik utama dalam pencatatan, pemantauan, dan penyajian data perkara penerapan prinsip-prinsip ISO 27001 dan KAMI menjadi sangat penting guna menjamin bahwa data perkara tetap aman, akurat, serta terlindungi dari ancaman siber. Dengan mengintegrasikan pendekatan sistematis dari ISO 27001 dan evaluasi berkelanjutan dari KAMI, Pengadilan Militer III-15 Kupang dapat mewujudkan pengelolaan SIPP yang andal, transparan, dan sesuai dengan prinsip *good governance* dalam pelayanan peradilan militer.

Berdasarkan hasil evaluasi terhadap penerapan ISO 27001, dapat disimpulkan bahwa organisasi telah menunjukkan tingkat kepatuhan yang cukup baik dalam menerapkan praktik keamanan informasi. Sebagian besar indikator telah diterapkan secara menyeluruh, khususnya pada aspek penyusunan dan pengelolaan kebijakan keamanan informasi, manajemen aset informasi, pengamanan layanan *cloud*, pengamanan teknologi termasuk pengembangan aplikasi yang aman, serta mekanisme perlindungan terhadap kebocoran data (*Data Leakage Prevention*). Selain itu, perencanaan dan pengujian pemulihan bencana (*disaster recovery*) juga telah dilaksanakan sesuai dengan ketentuan standar ISO 27001.

Namun, masih terdapat beberapa area yang memerlukan perhatian dan peningkatan lebih lanjut. Beberapa indikator masih berada pada tahap “dalam penerapan” atau “diterapkan sebagian”, terutama terkait proses penghancuran informasi yang tidak lagi dibutuhkan, pengamanan fisik terhadap fasilitas dan infrastruktur komputasi (termasuk perlindungan terhadap gangguan listrik dan akses fisik tidak sah), serta pengelolaan konfigurasi sistem dan pencatatan log aktivitas sistem secara otomatis.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil evaluasi menggunakan Indeks KAMI Versi 5.0 terhadap Sistem Informasi Penelusuran Perkara (SIPP) di Pengadilan Militer III-15 Kupang, dapat disimpulkan bahwa tingkat kesiapan keamanan informasi berada pada kategori cukup baik

dengan skor total 736 dan masuk dalam kategori SE tinggi. Evaluasi terhadap tujuh domain utama menunjukkan bahwa Kerangka Kerja Keamanan Informasi dan Pengelolaan Aset telah mencapai tingkat kematangan tertinggi (tingkat V), namun masih terdapat kekurangan pada domain Tata Kelola, Pengelolaan Risiko, dan Teknologi serta Keamanan Informasi yang masih berada di tingkat kematangan II, serta Perlindungan Data Pribadi (PDP) pada tingkat III. Oleh karena itu, disarankan agar organisasi memperkuat tata kelola keamanan informasi melalui kebijakan formal dan struktur pengelolaan yang jelas, meningkatkan pengelolaan risiko sesuai standar ISO 27005, serta memperkuat infrastruktur dan sistem keamanan teknologi informasi termasuk pencatatan log dan pemantauan insiden. Selain itu, perlindungan data pribadi perlu ditingkatkan seiring dengan regulasi yang berlaku, didukung oleh pelatihan SDM secara berkelanjutan dan peningkatan kesadaran keamanan informasi di seluruh organisasi. Evaluasi berkala melalui Indeks KAMI juga penting untuk dilakukan agar perbaikan keamanan informasi dapat terukur, konsisten, dan adaptif terhadap ancaman yang terus berkembang di era digital.

DAFTAR REFERENSI

Chazar, C. (2015). Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005. *Jurnal Informasi,* 7(2), 48-57. Retrieved from https://www.academia.edu/34436133/STANDAR_MANAJEMEN_KEAMANAN_SISTEM_INFORMASI_BERBASIS_ISO_27001

Khamil, D.I., Sasmita, A.M.G., & Susila, H.N.A.A. (2022). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar). *Jurnal Teknik Informatika dan Sistem Informasi*, 9(3), 1948-1960. Retrieved from https://jurnal.mdp.ac.id/index.php/jatisi/article/view/2310

Nurfadilah, D. R., Putra, W. H. N., & Rachmadi, A. (2020). Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001: 2013 (Studi Kasus: Aplikasi E-Kinerja). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *4*(9), 3014-3020. Retrieved from https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7845

Octariza, F.N. (2019). Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 pada Kantor Pusat PT Jasa Marga. Universitas Islam Negeri Syarif Hidayatullah Jakarta. Retrieved from https://repository.uinjkt.ac.id/dspace/handle/123456789/48163#:~:text=Penelitian%20ini%20membahas%20tentang%20analisis%20sistem%20manajemen%20keamanan,pengumpulan%2C%20analisis%2C%20dan%20pengolahan%20data%20yang%20telah%20ditemukan.

Rutanaji, D., Kusumawardani, S. S., & Winarno, W. W. (2018). Penggunaan Kerangka Kerja SNI ISO/IEC 27001: 2013 Untuk Implementasi Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan (Arsip Nasional RI). Seminar Nasional GEOTIK 2018.