PENGUKURAN TINGKAT KEMATANGAN TATA KELOLA KEAMANAN INFORMASI DI STMIK PALANGKARAYA DENGAN INDEKS KEAMANAN INFORMASI 5.0

Amaya Andri Damaini, Abdul Hadi, Elia Zakharia, Herkules
Teknik Informatika, STMIK Palangkaraya
Jl. G. Obos No.114, Menteng, Kec. Jekan Raya, Kota Palangka Raya, Kalimantan Tengah, Indonesia
amayaandridamaini@gmail.com

ABSTRAK

STMIK Palangkaraya memiliki ketergantungan tinggi terhadap teknologi informasi yang meningkatkan risiko keamanan informasi. Permasalahan utama meliputi belum optimalnya tata kelola, pengelolaan risiko, serta perlindungan data pribadi. Penelitian ini bertujuan mengukur tingkat kesiapan dan kematangan keamanan informasi menggunakan Indeks KAMI versi 5.0 serta memberikan rekomendasi berbasis ISO/IEC 27001:2022. Metode yang digunakan adalah deskriptif kualitatif melalui wawancara, observasi, kuesioner, dan analisis dokumen pada tujuh domain evaluasi. Hasil menunjukkan skor 154 dengan status "Tidak Layak" dan tingkat kematangan berada pada level I–II. Kelemahan utama terdapat pada tata kelola, manajemen risiko, dan kerangka kerja keamanan informasi, sementara pengamanan pihak ketiga relatif lebih baik. Penelitian ini merekomendasikan penyusunan kebijakan formal, penguatan manajemen risiko, peningkatan kontrol teknis, serta evaluasi berkala untuk meningkatkan keamanan informasi secara berkelanjutan.

Kata kunci : *Keamanan Informasi, Tata Kelola TI, Indeks KAMI, ISO/IEC 27001*

1. PENDAHULUAN

STMIK Palangkaraya, sebagai lembaga yang berfokus pada bidang informatika dan komputer, memiliki ketergantungan yang sangat tinggi terhadap infrastruktur TI untuk mendukung proses pembelajaran, penyimpanan data akademik, serta pengelolaan informasi strategis. Infrastruktur ini mencakup jaringan komunikasi, server penyimpanan data, sistem manajemen basis data, hingga berbagai perangkat lunak yang digunakan dalam operasional sehari-hari. Kemajuan teknologi yang pesat memunculkan tantangan baru berupa ancaman keamanan siber yang semakin canggih dan kompleks, seperti peretasan, malware, ransomware, dan phishing, yang dapat mengancam integritas, kerahasiaan, dan ketersediaan data [1].

Salah satu contoh insiden terjadinya pemalsuan akun WhatsApp yang terjadi di lingkungan STMIK Palangkaraya. Pelaku kejahatan mengganti foto profil menyerupai kenalan korban dan mengirim pesan palsu kepada rekan kerja dengan menyebut nama lengkap korban. Insiden ini mengindikasikan adanya kebocoran data identitas korban.

Dalam konteks pendidikan tinggi, insiden keamanan ini tidak hanya dapat menyebabkan kerugian finansial yang signifikan, tetapi juga dapat mengancam privasi data mahasiswa, merusak reputasi institusi, serta menghambat kelancaran proses akademik dan administratif [2].

Selain itu, kebijakan keamanan yang tidak memadai, kurangnya kesadaran pengguna terhadap risiko keamanan, serta kelemahan dalam implementasi prosedur keamanan, sering kali menjadi celah yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab[3].

Tata kelola keamanan TI yang baik menjadi prasyarat utama bagi STMIK Palangkaraya untuk beroperasi secara efektif dan aman. Ini mencakup pengelolaan risiko, kepatuhan terhadap regulasi, serta pemantauan dan evaluasi berkala. Untuk mencapainya, diperlukan pemahaman mendalam atas kondisi keamanan saat ini, identifikasi potensi risiko, dan asesmen komprehensif guna mengukur efektivitas kebijakan serta prosedur yang ada [4], [5].

Penelitian ini bertujuan menilai tata kelola keamanan TI di STMIK Palangkaraya menggunakan Indeks Keamanan Informasi versi 5, dengan harapan dapat menjadi panduan dalam merumuskan strategi keamanan yang tangguh dan berkelanjutan. Selain memberikan gambaran kondisi tata kelola keamanan TI saat ini, penelitian ini juga menghasilkan rekomendasi praktis untuk memperkuat sistem keamanan informasi.

Indeks Keamanan Informasi (KAMI) merupakan alat asesmen dengan kerangka kerja sistematis untuk menilai tingkat kematangan tata kelola keamanan informasi suatu organisasi [6], [7].

Alat ini dipilih karena adaptif terhadap kebutuhan institusi, termasuk pendidikan [8], pemerintahan [9], maupun perusahaan skala nasional [10] [11], sehingga mampu mengidentifikasi kelemahan sistem secara komprehensif, memberikan penilaian terukur, meningkatkan efektivitas tata kelola TI, dan menetapkan langkah perbaikan untuk meningkatkan keamanan informasi secara menyeluruh.

Meskipun berbagai penelitian telah menggunakan Indeks KAMI untuk mengukur keamanan informasi, masih terbatas kajian yang secara spesifik mengevaluasi institusi pendidikan tinggi.

Oleh karena itu, penelitian ini penting untuk memberikan gambaran empiris serta rekomendasi strategis yang kontekstual.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Beberapa penelitian sebelumnya menunjukkan bahwa Indeks KAMI telah diterapkan secara luas di sektor publik. Salah satunya adalah penelitian yang mengkaji penerapan Indeks KAMI versi 4.1 sebagai alat evaluasi dalam menilai tingkat kesiapan keamanan informasi pada PT. BPR Jawa Timur. Hasil dari penelitian tersebut menunjukkan bahwa PT. BPR Jatim secara umum telah memiliki tingkat kematangan yang tinggi, terutama pada area perlindungan data pribadi dan pengamanan pihak ketiga. Aspek teknologi dan pengelolaan aset juga dinilai telah memenuhi kerangka kerja dasar, penerapan operasional, serta kepatuhan terhadap standar ISO/SNI 27001. Meskipun demikian, masih ditemukan kelemahan pada aspek tata kelola dan manajemen risiko, yang hanya memenuhi kerangka kerja dasar dan belum mencapai tingkat kepatuhan terhadap standar internasional. Selain itu, aspek kerangka kerja organisasi dinilai belum memenuhi standar dalam tiga level yang ditentukan: kerangka kerja dasar, operasional, maupun kepatuhan [10].

Maryanto dan Nugroho dalam penelitiannya melakukan evaluasi pada perusahaan pemula berbasis teknologi dan menemukan bahwa ketiga area utama keamanan informasi berada pada tingkat "Tidak Layak" (Level I – I+). Mayoritas indikator belum diterapkan, dan rekomendasi diberikan merujuk pada ISO 27002:2013, seperti penyusunan prosedur pertukaran informasi yang aman [11].

Penelitian lain mengevaluasi keamanan informasi di Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Gianyar menggunakan Indeks KAMI versi 4.2. Penelitian ini bertujuan untuk menilai tingkat kesiapan keamanan informasi dalam menjaga kerahasiaan, integritas, dan keaslian data, sesuai dengan Peraturan BSSN No. 8 Tahun 2021. Hasil evaluasi menunjukkan bahwa DISKOMINFO Gianyar memperoleh skor akhir sebesar 190 dengan status "Tidak Layak" untuk memenuhi standar ISO/IEC 27001:2013. Penelitian ini juga membandingkan hasil evaluasi dengan kontrol ISO 27001 dan memberikan rekomendasi perbaikan terhadap aspek-aspek yang belum memenuhi standar. Studi ini menunjukkan pentingnya penerapan Indeks KAMI sebagai alat evaluasi standar dalam lembaga pemerintah daerah, sekaligus menegaskan perlunya peningkatan pengelolaan keamanan informasi agar sejalan dengan standar internasional [9].

Sementara itu, penelitian lain di UIN Sunan Kalijaga Yogyakarta menjadi contoh penerapan Indeks KAMI di sektor pendidikan tinggi. Dengan skor awal 407, implementasi OSSIM (Open Source SIEM) berhasil meningkatkan skor menjadi 432. Meskipun terjadi peningkatan skor, hasil akhir tetap berada pada tingkat kematangan I+ sampai II+, sehingga dinilai masih belum layak dan perlu perbaikan berkelanjutan [8].

Berdasarkan kajian penelitian sebelumnya, Indeks Keamanan Informasi (KAMI) telah digunakan secara luas untuk mengukur tingkat kematangan keamanan informasi pada berbagai sektor, seperti perbankan, startup, pemerintahan, dan pendidikan tinggi. Namun, sebagian besar penelitian masih menggunakan Indeks KAMI versi 4.x dan mengacu pada standar ISO/IEC 27001:2013, serta cenderung hanya berfokus pada evaluasi tanpa integrasi strategis terhadap peningkatan berkelanjutan. Selain itu, kajian pada sektor pendidikan tinggi masih terbatas dan menunjukkan tingkat kematangan yang relatif rendah. Oleh karena itu, penelitian ini hadir sebagai pengembangan dengan menggunakan Indeks KAMI versi 5.0 yang lebih mutakhir serta mengintegrasikan hasil asesmen dengan standar ISO/IEC 27001:2022. Kebaruan penelitian ini terletak pada pendekatan evaluatif dan preskriptif yang tidak hanya mengukur tingkat kematangan, tetapi juga merumuskan arah peningkatan berbasis domain secara sistematis.

2.2. Keamanan Informasi

Keamanan informasi merupakan bidang krusial di era digital yang bertujuan melindungi data dari ancaman perusakan, pencurian, atau pengungkapan tanpa izin. Konsep ini berlandaskan tiga prinsip utama CIA Triad: kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) [12].

Kerahasiaan dapat dijaga melalui enkripsi dan kontrol akses; integritas dipastikan dengan *hash function* [13] dan tanda tangan digital [14]; sedangkan ketersediaan dilindungi dari serangan seperti DoS melalui *backup* dan pemulihan bencana. Ancaman dapat berasal dari internal maupun eksternal, termasuk serangan *phishing* dan *social engineering* [15], sehingga pendidikan keamanan menjadi langkah preventif penting.

Berbagai model keamanan, seperti Bell-LaPadula [16] untuk kerahasiaan, Biba [17] dan Clark-Wilson [18] untuk integritas juga digunakan bersama standar internasional seperti ISO/IEC 27001 [19][20], NIST *Cybersecurity Framework* , dan COBIT[21] [22].

Perkembangan teknologi seperti cloud computing, IoT, dan AI memunculkan ancaman baru, misalnya kerentanan perangkat IoT, yang menuntut pembaruan strategi keamanan. Dalam menghadapi semua tantangan ini, organisasi harus menerapkan praktik terbaik dalam keamanan informasi, seperti melakukan audit keamanan secara berkala, mengedukasi karyawan tentang ancaman keamanan, dan mengadopsi teknologi keamanan terbaru. Dengan demikian, risiko yang terkait dengan keamanan informasi dapat dikurangi dan aset informasi terlindungi dengan lebih baik.

2.3. Indeks Keamanan Informasi (KAMI)

Indeks KAMI merupakan alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan [7].

Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013. Hasil evaluasi ini dapat digunakan secara berkala untuk mendapatkan gambaran kelengkapan dan kematangan kerangka kerja keamanan informasi, yang dapat digunakan sebagai acuan penyusunan prioritas perbaikan dan pemantauan perkembangan dari waktu ke waktu [6].

Proses evaluasi Indeks KAMI dilakukan melalui serangkaian pertanyaan pada tujuh area: (a) kategori Sistem Elektronik, (b) tata kelola keamanan informasi, (c) pengelolaan risiko, (d) kerangka kerja keamanan informasi, (e) pengelolaan aset informasi, (f) teknologi dan keamanan informasi, serta (g) suplemen, yang mencakup pengamanan pihak ketiga, layanan cloud, dan perlindungan data pribadi [23].

Jawaban harus mencerminkan kondisi nyata penerapan keamanan informasi, dengan asas keterbukaan dan kejujuran untuk memastikan hasil yang bermanfaat.

Sebelum menjawab, responden mendefinisikan kategori Sistem Elektronik di instansinya—rendah, tinggi, atau strategis—serta mendeskripsikan infrastruktur TIK secara singkat. Pengelompokan ini memudahkan pemetaan instansi dengan karakteristik serupa.

Pertanyaan disusun untuk dua tujuan: mengukur kelengkapan kontrol sesuai ISO/IEC 27001:2013 dan menilai kematangan penerapan [24].

Tanggapan diberi label '1' untuk kerangka kerja dasar, '2' untuk efektivitas dan konsistensi penerapan, dan '3' untuk kemampuan peningkatan berkelanjutan. Tingkat kematangan dibagi menjadi lima level: I (awal), II (kerangka kerja dasar), III (terdefinisi dan konsisten), IV (terkelola dan terukur), dan V (optimal).

3. METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif dengan fokus pada penerapan Indeks Keamanan Informasi (KAMI) versi 5.0 sebagai instrumen evaluasi. Pendekatan ini bertujuan untuk menggambarkan serta menganalisis tingkat kesiapan dan kematangan keamanan informasi secara mendalam, tanpa bergantung semata pada data kuantitatif. Melalui metode ini, penelitian tidak hanya menilai parameter keamanan berdasarkan standar Indeks KAMI, tetapi juga memahami konteks kebijakan, praktik, serta faktor internal maupun eksternal yang memengaruhi penerapannya.

3.1. Teknik Pengumpulan Data

Data dikumpulkan dengan beberapa teknik kualitatif, yaitu:

a. Wawancara, dilakukan dengan admin TI dan pihak manajemen STMIK Palangkaraya untuk menggali informasi terkait kebijakan, tantangan, dan persepsi keamanan informasi.
b. Analisis dokumen, mencakup telaah SOP pengelolaan TI, kontrak layanan pihak ketiga, serta dokumen lain yang berkaitan dengan tata kelola keamanan.
c. Observasi lapangan, meliputi pengamatan langsung terhadap penggunaan sistem SMART, pengelolaan akses jaringan melalui Access Point, server lokal website kampus, serta pengamanan fisik perangkat keras TI.

3.2. Tahapan Penelitian

Tahapan penelitian ini terdiri dari empat langkah utama seperti pada Gambar 1.

Gambar 1. Tahapan penelitian

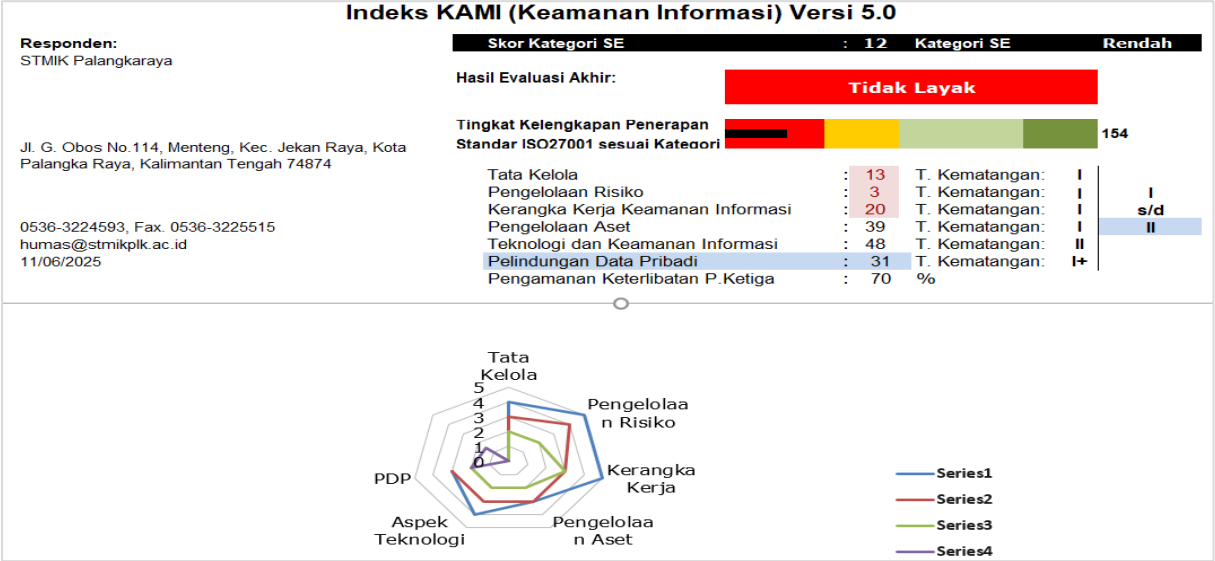
Berikut penjelasan tahapan penelitian:

a. Tahap persiapan, yaitu melakukan studi literatur, telaah dokumen TIK dan hasil audit sistem informasi di STMIK Palangkaraya, serta identifikasi awal permasalahan keamanan informasi.

b. Tahap desain penelitian, yang mencakup identifikasi organisasi, perumusan batasan masalah, serta pengisian instrumen Indeks Keamanan Informasi (KAMI) versi 5.0 sebagai alat evaluasi.
c. Tahap pengumpulan dimana data diperoleh melalui wawancara, observasi, dan analisis dokumen, kemudian diolah berdasarkan parameter Indeks KAMI.
d. Analisis dilakukan pada tujuh area penilaian dengan dua dimensi utama: tingkat kelengkapan kontrol (label 1–3) dan tingkat kematangan penerapan (level I–V). Hasil analisis ini digunakan untuk menentukan skor kesiapan keamanan informasi mengidentifikasi kelemahan, serta merumuskan rekomendasi perbaikan.
e. Tahap pelaporan, yang berfokus pada penyajian hasil asesmen berupa skor kesiapan keamanan informasi, interpretasi tingkat kematangan di setiap domain, serta perumusan rekomendasi praktis yang dapat diimplementasikan oleh institusi untuk memperkuat tata kelola keamanan informasi.

4. HASIL DAN PEMBAHASAN

Asesmen keamanan informasi di STMIK Palangkaraya menggunakan Indeks KAMI versi 5.0 menghasilkan skor total 154, yang menempatkan institusi pada kategori “Tidak Layak” untuk standar ISO/IEC 27001. Hasil pengukuran tingkat kematangan tata kelola keamanan informasi di tujuh domain utama terdapat pada Gambar 2.



Gambar 2. Hasil Asesmen Secara Umum di Linkungan STMIK Palangkaraya

4.1. Sistem Elektronik

Berdasarkan Tabel 1, pengelolaan Sistem Elektronik di STMIK Palangkaraya masih tergolong rendah. Sebagian besar butir asesmen berstatus C (skor 1), menunjukkan bahwa praktik pengelolaan, pemanfaatan, dan perlindungan sistem elektronik belum memadai. Nilai investasi masih di bawah Rp 3 miliar dan anggaran operasional kurang dari Rp 1 miliar, sehingga penerapan kriptografi untuk perlindungan data belum dilakukan.

Tabel 1. Hasil Asesmen Sistem Elektronik

Kategori	Jumlah Pertanyaan	Total Skor
A	0	0
B	2	4
C	8	8
Total	**10**	**12**

Selain itu, regulasi internal terkait kepatuhan terhadap PP No. 71 Tahun 2019 dan UU No. 27 Tahun 2022 belum tersedia, padahal kedua regulasi tersebut mewajibkan penerapan prinsip keamanan dan perlindungan data pribadi dalam sistem elektronik [25], [26]. Tidak adanya klasifikasi data menyebabkan data pribadi dosen dan pejabat struktural rentan disalahgunakan, sebagaimana terlihat dari kasus penyalahgunaan identitas pejabat STMIK Palangkaraya. Kondisi ini menimbulkan risiko reputasional, hukum, dan finansial.

Oleh karena itu, penerapan mekanisme kriptografi seperti tanda tangan digital RSA dan enkripsi data [27] serta sistem klasifikasi dan manajemen risiko data sesuai PP 71/2019 dan UU PDP 2022 menjadi kebutuhan mendesak. Dua indikator dengan status B, yaitu jumlah pengguna dan pengelolaan data pribadi menunjukkan sistem sudah dimanfaatkan luas, namun tata kelola keamanannya belum sepadan dengan skala penggunaannya.

Peningkatan sistem elektronik di STMIK Palangkaraya perlu difokuskan pada evaluasi investasi dan anggaran agar mendukung strategi digitalisasi, pembentukan Tim Pengawasan dan Kepatuhan

Regulasi untuk memastikan kepatuhan terhadap PP No. 71/2019 dan UU PDP 2022, serta penerapan enkripsi data dengan algoritma kriptografi yang diakui. Selain itu, diperlukan klasifikasi data dan proses bisnis berdasarkan tingkat dampaknya serta penilaian risiko komprehensif guna mengidentifikasi potensi kerugian akibat insiden keamanan. Implementasi langkah-langkah ini diharapkan dapat meningkatkan kematangan pengelolaan sistem elektronik menuju kesesuaian dengan standar ISO/IEC 27001.

4.2. Tata Kelola Keamanan Informasi

Berdasarkan Tabel 2, tingkat tata kelola keamanan informasi di STMIK Palangkaraya berada di tingkat kematangan I+ dengan total skor 13 dari 22 butir asesmen.

Tabel 2. Hasil Asesmen Tata Kelola Keamanan Informasi

Tingkat Keamanan	Tingkat Kematangan				Total Skor
	II	III	IV	V	
Tk. 1	11	2	–	–	13
Tk. 2	–	–	–	–	0
Tk. 3	–	–	–	–	0
Total Skor	11	2	0	0	13
Tk. Kematangan	I+ (Dalam Perencanaan / Awal Penerapan)				

Berdasarkan Tabel 3, Sebagian besar (73%) kegiatan terutama pada tingkat II dan IV masih berada pada status “Tidak Dilakukan”, yang menandakan area penguatan kebijakan dan peran pelaksana keamanan informasi masih perlu dikembangkan. Hanya 3 kontrol (14%) yang sudah mencapai tahap “Dalam Penerapan”, dan belum ada yang diterapkan secara menyeluruh. Padahal, keamanan informasi merupakan bagian integral dari tata kelola organisasi, bukan sekadar tanggung jawab teknis. Kondisi ini menyebabkan keamanan informasi belum terintegrasi dalam proses kerja organisasi, termasuk perlindungan data pribadi, serta belum adanya mekanisme monitoring, evaluasi, pelaporan, dan penanganan insiden. Situasi ini menempatkan tata kelola pada risiko tinggi terhadap kebocoran dan ketidakpatuhan regulasi.

Tabel 3. Status penerapan Tata Kelola Keamanan Informasi

Status	Tingkat Kematangan				Total
	II	III	IV	V	
Tidak Dilakukan	8	2	6	0	16
Dalam Perencanaan	2	1	0	0	3
Dalam Penerapan / Diterapkan Sebagian	3	0	0	0	3
Diterapkan Secara Menyeluruh	0	0	0	0	0
Total Pertanyaan	**13**	**3**	**6**	**0**	**22**

Oleh karena itu, untuk perbaikan diperlukan langkah-langkah strategis seperti: manajemen dan pimpinan lembaga harus mengambil peran aktif dalam memastikan perlindungan data sebagai aset penting organisasi [28]. Hal ini dapat dilakukan dengan penetapan kebijakan resmi dan penanggung jawab melalui SK pimpinan. Selain itu, integrasi kontrol keamanan secara berkelanjutan untuk memperkuat sistem keamanan informasi secara menyeluruh penting untuk dilakukan [29]. Ini dapat diwujudkan dengan penyediaan sumber daya dan pelatihan SDM, serta sosialisasi dan integrasi prinsip keamanan informasi dalam proses bisnis. Selain itu, perlu dibentuk Tim Pengawas Kepatuhan Keamanan Informasi guna memastikan pelaporan berkala, penilaian kinerja, dan penanganan insiden sesuai regulasi. Penerapan rekomendasi ini diharapkan memperkuat tata kelola dan meningkatkan tingkat kematangan keamanan informasi institusi.

4.3. Pengelolaan Risiko Keamanan Informasi

Tingkat kematangan pengelolaan risiko keamanan informasi seperti terdapat pada Tabel 4 berada pada kategori I (Awal/BelumValid). Dengan total skor 3 poin menggambarkan bahwa organisasi masih dalam tahap membangun kerangka dasar pengelolaan risiko keamanan informasi.

Tabel 4. Hasil Asesmen Risiko Keamanan Informasi

Tingkat Keamanan	Tingkat Kematangan				Total Skor
	II	III	IV	V	
Tk. 1	1	–	–	–	1
Tk. 2	–	2	–	–	2
Tk. 32	–	–	–	–	0
Total Skor	1	2	0	0	3
Tk. Kematangan	I (Dalam Perencanaan / Awal Penerapan)				

Status penerapan pada Tabel 5 menunjukkan dari total 16 butir kontrol dalam domain Pengelolaan Risiko Keamanan Informasi, hanya 13 pertanyaan yang dianggap valid untuk perhitungan tingkat kematangan, sesuai ketentuan Indeks KAMI bahwa tahap penerapan dengan status tidak valid (Tahap 3) harus dikecualikan. Tahap 3 dinyatakan tidak valid karena skor aktual 3 tidak mencapai batas minimal 40 poin.

Tabel 5. Status Penerapan Risiko Keamanan Informasi

Status	Tingkat Kematangan				Total
	II	III	IV	V	
Tidak Dilakukan	9	2	-	-	11
Dalam Perencanaan	1	1	-	-	2
Dalam Penerapan / Diterapkan Sebagian	0	0	-	-	0
Diterapkan Secara Menyeluruh	0	0	-	-	0
Total Pertanyaan Valid	**10**	**3**	**0**	**0**	**13**

Sebagian besar kontrol (lebih dari 80%) berada pada status "Tidak Dilakukan", menandakan bahwa organisasi belum memiliki mekanisme manajemen risiko keamanan informasi yang terdokumentasi dan berfungsi secara formal. Aktivitas terkait identifikasi risiko, mitigasi, serta evaluasi efektivitas pengendalian belum terdefinisi dan belum menjadi bagian dari kebijakan atau prosedur institusi. Menurut ISO/IEC 27005 [30], organisasi perlu memiliki program kerja risiko yang terdokumentasi untuk mengidentifikasi, menilai, dan menangani risiko secara sistematis. Selain itu, penetapan penanggung jawab risiko dan jalur pelaporan ke pimpinan penting agar respons terhadap ancaman dapat dilakukan cepat dan tepat [31]. Dukungan pimpinan juga berperan besar dalam membangun budaya keamanan informasi yang efektif [32].

Terdapat dua kontrol yang berada dalam tahap "Dalam Perencanaan" menandakan mulai adanya inisiatif penyusunan langkah mitigasi dan penentuan prioritas risiko.

Untuk itu, disarankan agar institusi menyusun kerangka kerja pengelolaan risiko, menetapkan penanggung jawab dan jalur eskalasi, serta melaksanakan identifikasi aset, analisis risiko, mitigasi, dan evaluasi berkala yang diintegrasikan dengan kinerja keamanan informasi organisasi.

4.4. Kerangka kerja Pengelolaan Keamanan Informasi

Berdasarkan hasil asesmen pada tabel 6, tingkat kematangan domain ini dikategorikan pada tingkat I+. Total skor yang diperoleh sebesar 20, dengan distribusi nilai menunjukkan adanya beberapa kontrol yang telah berada pada Tingkat Kematangan II dan III. Meskipun demikian, total skor tersebut masih berada di bawah ambang batas minimum yang ditetapkan untuk validasi tingkat kematangan tahap penerapan yaitu 68.

Tabel 6. Hasil Asesmen Kerangka kerja Pengelolaan Keamanan Informasi

Tingkat Keamanan	**Tingkat Kematangan**				**Total Skor**
	II	**III**	**IV**	**V**	
Tk. 1	0	2	–	–	4
Tk. 2	4	14	–	–	16
Tk. 3	–	–	–	–	0
Total Skor	4	16	0	0	20
Tk. Kematangan	I (Dalam Perencanaan / Awal Penerapan)				

Dengan demikian, dari total 33 kontrol yang dievaluasi pada Tabel 7, hanya 21 butir yang dinyatakan valid dari tahap penerapan 1 dan 2. Sebanyak 14 butir kontrol masih pada status "Tidak Dilakukan", dan 4 butir kontrol sudah berada di tahap "Dalam Perencanaan". Hanya masing-masing 1 kontrol yang mencapai tahap penerapan (baik sebagian maupun menyeluruh).

Tabel 7. Status Penerapan Kerangka Kerja Pengelolaan Keamanan Informasi

Status	**Tingkat Kematangan**				**Total**
	II	**III**	**IV**	**V**	
Tidak Dilakukan	8	6	-	-	14
Dalam Perencanaan	0	4	-	-	4
Dalam Penerapan / Diterapkan Sebagian	1	1	-	-	2
Diterapkan Secara Menyeluruh	0	1	-	-	1
Total Pertanyaan Valid	**9**	**1**2	**0**	**0**	**21**

Hasil ini mengindikasikan bahwa organisasi telah menunjukkan adanya upaya awal dalam membangun kerangka kerja pengelolaan keamanan informasi, namun belum ada SOP penanganan insiden, aturan keamanan dengan pihak ketiga, atau fungsi *threat intelligence* yang aktif [33].

Selain itu, rencana keberlangsungan layanan dan pemulihan bencana belum tersedia, serta audit dan evaluasi keamanan masih dalam tahap perencanaan.

Untuk mencapai tingkat kematangan berikutnya, organisasi perlu memperkuat proses penyusunan dan penerapan kebijakan formal, memastikan adanya mekanisme evaluasi dan tindak lanjut hasil audit, serta meningkatkan konsistensi penerapan standar keamanan informasi di seluruh unit kerja[31].

Selain itu, pelaksanaan evaluasi berkala dan dokumentasi hasil penerapan menjadi langkah penting untuk memastikan keberlanjutan dan efektivitas pengelolaan keamanan informasi di masa mendatang.

4.5. Pengelolaan Aset Informasi

Berdasarkan hasil asesmen pengelolaan aset informasi pada tabel 8, dari total 53 butir pertanyaan, hanya 46 pertanyaan yang dinyatakan valid untuk dihitung. Hal ini disebabkan karena tahap penerapan ke-3 dinyatakan tidak valid akibat nilai yang diperoleh belum mencapai batas skor minimal sebesar 130 poin.

Tabel 8. Status Penerapan Pengelolaan Aset Informasi

Status	**Tingkat Kematangan**				**Total**
	II	**III**	**IV**	**V**	
Tidak Dilakukan	18	14	-	-	32
Dalam Perencanaan	4	1	-	-	5
Dalam Penerapan / Diterapkan Sebagian	6	1	-	-	7
Diterapkan Secara Menyeluruh	4	2	-	-	6
Total Pertanyaan Valid	32	18	**0**	0	46

Dengan demikian, analisis tingkat kematangan dilakukan hanya pada tahap 1 dan tahap 2, yang mencakup aspek-aspek pengelolaan aset informasi, pengendalian akses, pengamanan fisik, serta kebijakan penggunaan sistem informasi. Dari 46 kontrol yang

dievaluasi, diperoleh total skor sebesar 39 poin, dengan rincian 31 poin pada tingkat kematangan II dan 8 poin pada tingkat kematangan III. Hasil asesmen pada Tabel 9 menunjukkan bahwa domain Pengelolaan Aset Informasi berada pada Tingkat Kematangan II (Dalam Perencanaan/Awal Penerapan).

Secara umum, capaian ini mengindikasikan bahwa institusi telah mulai membangun kesadaran dan struktur awal pengelolaan aset informasi, namun sebagian besar kontrol masih berada pada tahap perencanaan dan belum sepenuhnya diterapkan secara konsisten. Selain itu, prosedur *backup* dan *restore* belum terdokumentasi dengan baik, sementara penggunaan layanan *cloud* belum disertai kajian risiko dan kebijakan keamanan. Beberapa pengamanan fisik seperti kontrol akses dan listrik cadangan telah diterapkan, namun perlindungan berlapis terhadap ruang server belum tersedia.

Tabel 9. Hasil Asesmen Pengelolaan Aset Informasi

Tingkat Keamanan	**Tingkat Kematangan**				**Total Skor**
	II	**III**	**IV**	**V**	
Tk. 1	31	8	0	–	39
Total Skor	31	8	0	0	39
Tk. Kematangan	II (Dalam Perencanaan / Awal Penerapan)				

Oleh karena itu, direkomendasikan penerapan *Role-Based Access Control* (RBAC) untuk peningkatan area pengendalian akses [34]. Peningkatan pengamanan fisik berlapis, penyusunan prosedur backup dan manajemen log, serta penerapan enkripsi dan kebijakan komunikasi aman agar perlindungan aset informasi menjadi lebih efektif dan sesuai standar internasional.

4.6. Teknologi dan Keamanan Informasi

Berdasarkan Tabel 10, hasil asesmen menunjukkan bahwa pengelolaan teknologi dan keamanan informasi Memperoleh skor total 48 poin dari 29 kontrol valid yang diukur pada tahap 1 dan 2. Hasil ini menempatkan tingkat kematangan pada Level II (Dalam Perencanaan / Awal Penerapan).

Tabel 10. Hasil Asesmen Teknologi dan Keamanan Informasi

Tingkat Keamanan	**Tingkat Kematangan**				**Total Skor**
	II	**III**	**IV**	**V**	
Tk. 1	28	20	–	–	48
Tk. 2	–	–	–	–	0
Tk. 3	–	–	–	–	0
Total Skor	28	0	0	0	13
Tingkat Kematangan	**II (Dalam Perencanaan / Awal Penerapan)**				

Status penerapan teknologi dan keamanan informasi pada Tabel 11 menunjukkan sebagian besar kontrol (20 butir) berada pada kategori “Tidak Dilakukan”, sementara hanya sebagian kecil yang “Diterapkan Secara Menyeluruh” (8 butir), seperti segmentasi jaringan dan perlindungan *malware*. Hal ini menunjukkan lemahnya tata kelola lanjutan, termasuk belum adanya praktik seperti review keamanan aplikasi, validasi fungsional, dan *Data Leakage Prevention* (DLP).

Tabel 11. Status Penerapan Teknologi dan Keamanan Informasi

Status	**Tingkat Kematangan**		**Total Kontrol Valid**
	II	**III**	
Tidak Dilakukan	10	10	20
Dalam Perencanaan	0	0	0
Dalam Penerapan / Diterapkan Sebagian	8	3	11
Diterapkan Secara Menyeluruh	4	4	8
Total Pertanyaan Valid	22	17	29
Skor Total Valid	**28**	**20**	**48**

Aspek penting lain masih lemah, terutama konfigurasi sistem, manajemen perubahan, dan analisis log keamanan, yang seharusnya dilakukan secara rutin sesuai ISO/IEC 27001. Selain itu, enkripsi dan manajemen kunci belum diterapkan, padahal ISO/IEC 27018 mewajibkan enkripsi data pribadi, terutama di layanan *cloud*. Pengelolaan identitas dan akses juga belum memenuhi standar karena tidak adanya kebijakan *password* kuat atau autentikasi berlapis. Dalam pengembangan aplikasi, belum diterapkan secure coding (mis. OWASP Top 10), source code review, maupun audit eksternal sebagaimana disyaratkan oleh ISO/IEC 27001 Klausul 9.2.

Untuk peningkatan, disarankan memprioritaskan perbaikan kontrol dasar, mengidentifikasi celah keamanan, dan meningkatkan investasi teknologi melalui penerapan enkripsi dan manajemen kunci, logging dan *audit trail*, *secure coding*, serta mekanisme DLP dengan keterlibatan pihak independen untuk audit keamanan berkala.

4.7. Pelindungan Data Pribadi (PDP)

Domain Pelindungan Data Pribadi yang disajikan dalam tabel 12 memperoleh total skor 31 poin dari 16 kontrol valid yang dinilai pada tahap penerapan 1 dan 2. Tahap penerapan ke-3 dinyatakan tidak valid karena skor aktual belum mencapai batas minimal 56 poin, sehingga tidak diperhitungkan dalam penentuan tingkat kematangan. Hasil tersebut menempatkan institusi pada Tingkat Kematangan I+ (Awal Perencanaan / Menuju Penerapan).

Tabel 12. Hasil Asesmen Pelindungan Data Pribadi (PDP)

Tingkat Keamanan	Tingkat Kematangan				Total Skor
	II	III	IV	V	
Tk. 1	9	22	–	–	31
Tk. 2	–	–	–	–	0
Tk. 3	–	–	–	–	0
Total Skor	9	22	0	0	31
Tingkat Kematangan	**I+ (Awal Perencanaan / Menuju Penerapan)**				

Dari 16 kontrol yang dinilai, ada 8 kontrol (50%) yang belum diterapkan sama sekali. Hal ini berarti belum ada kebijakan atau prosedur yang jelas untuk melindungi data pribadi, seperti pemetaan alur pengolahan data, penunjukan pejabat pelindung data pribadi, dan mekanisme pelaporan jika terjadi kebocoran data. Kondisi ini menunjukkan bahwa instansi masih berada pada tahap awal dalam membangun sistem pengelolaan data pribadi yang sesuai dengan aturan yang berlaku.

Sebanyak 4 kontrol (25%) sudah mulai diterapkan sebagian, misalnya dalam hal pencatatan data pribadi, analisis risiko, dan penghapusan data pribadi. Namun, penerapannya belum konsisten di semua bagian dan belum memiliki prosedur baku yang terdokumentasi.

Sementara itu, 4 kontrol lainnya (25%) sudah diterapkan dengan baik. Hal ini terlihat dari adanya dokumentasi proses pengelolaan data pribadi, sosialisasi kepada pegawai, serta penerapan mekanisme persetujuan dan pemutakhiran data. Capaian ini menjadi langkah positif karena menunjukkan adanya komitmen awal terhadap pelindungan data pribadi.

Untuk meningkatkan tingkat kematangan pelindungan data pribadi, instansi perlu segera menyusun kebijakan yang sesuai dengan peraturan, menetapkan pejabat khusus *Data Protection Officer* (DPO), serta meningkatkan pemahaman pegawai melalui pelatihan rutin. Selain itu, perlu diperkuat mekanisme audit, pelaporan, dan penghapusan data pribadi agar seluruh proses pengelolaan data berjalan aman, terpantau, dan sesuai dengan ketentuan hukum yang berlaku.

4.8. Suplemen (Pengamanan Keterlibatan Pihak Ketiga)

Berdasarkan Tabel 13, hasil asesmen Suplemen (Pengamanan Keterlibatan Pihak Ketiga) menunjukkan skor 59 dari 81 atau 70%. Nilai ini menandakan bahwa sebagian besar kontrol dalam domain ini telah berjalan baik, terutama pada aspek komunikasi risiko, pengelolaan subkontraktor, dan rencana kelangsungan layanan. Beberapa kontrol bahkan sudah diterapkan sepenuhnya, seperti pengelolaan alih daya, pelaporan insiden keamanan, serta kebijakan perubahan dan kelangsungan layanan pihak ketiga.

Meskipun demikian, masih terdapat beberapa aspek yang belum sepenuhnya diterapkan, terutama pada kebijakan formal keamanan pihak ketiga, audit keamanan TI, serta dokumentasi hasil pemantauan dan evaluasi. Kondisi ini menunjukkan bahwa penerapan pengelolaan keamanan pihak ketiga masih berada pada tingkat kematangan II menuju III (Dalam Penerapan Menuju Konsisten), di mana sebagian besar praktik telah berjalan, namun belum seluruhnya terdokumentasi atau diaudit secara berkala.

Untuk meningkatkan tingkat kematangan, institusi disarankan memperkuat kebijakan dan perjanjian kerja sama yang memuat klausul keamanan informasi secara lebih rinci, menetapkan mekanisme audit rutin terhadap kepatuhan pihak ketiga, serta meningkatkan koordinasi dalam tindak lanjut hasil pemantauan dan pelaporan insiden. Dengan langkah-langkah tersebut, tingkat kematangan keamanan informasi pada hubungan kerja sama dengan pihak ketiga dapat ditingkatkan menuju level "Diterapkan Secara Menyeluruh".

Tabel 13. Hasil Asesmen Suplemen

Aspek yang Dinilai	Jumlah Kontrol Valid	Skor Aktual	Skor Maksimal	Persentase Capaian (%)	Tingkat Kematangan	Status Validitas
Pengelolaan Risiko & Keamanan Pihak Ketiga	7	11	18	61%	II	Valid
Pengelolaan Sub-Kontraktor / Alih Daya	3	9	9	100%	III	Valid
Pengelolaan Layanan & Keamanan Pihak Ketiga	8	13	24	54%	II	Valid
Pengelolaan Perubahan dan Kebijakan	2	6	6	100%	III	Valid
Penanganan Aset dan Insiden	4	11	12	92%	III	Valid
Rencana Kelangsungan Layanan Pihak Ketiga	3	9	12	75%	III	Valid
Total / Rata-rata Domain	**27**	**59**	**81**	**70%**	**II–III**	

4.9. Rekapitulasi Hasil Asesmen dan Arah Peningkatan Menuju ISO/IEC 27001

Hasil rekapitulasi pada Tabel 14 menunjukkan bahwa sebagian besar domain keamanan informasi di STMIK Palangkaraya masih berada pada tingkat kematangan I–II, dengan fokus peningkatan yang dapat diarahkan pada penerapan kontrol sesuai ISO/IEC 27001:2022.

Domain Sistem Elektronik perlu diperkuat melalui implementasi kontrol terkait kebijakan penggunaan sistem, enkripsi, dan autentikasi. Pada Tata Kelola, langkah peningkatan diarahkan pada Klausul 5 dan A.5.1–A.5.3 untuk kepemimpinan dan kebijakan formal keamanan informasi. Pengelolaan Risiko memerlukan penerapan Klausul 6.1.2–6.1.3 guna membangun proses penilaian dan mitigasi risiko berbasis ISO/IEC 27005. Kerangka Kerja diarahkan ke Klausul 7 dan 9 untuk dukungan, evaluasi, serta komunikasi keamanan informasi. Pengelolaan Aset dan Teknologi dapat diperkuat melalui kontrol A.5.9–A.5.17 dan A.8.1–A.8.25, sedangkan Pelindungan Data Pribadi diselaraskan dengan A.5.34 dan ISO/IEC 27701:2019. Terakhir, Pengamanan Pihak Ketiga memerlukan penerapan A.5.19–A.5.21 yang mengatur manajemen hubungan dan audit keamanan pemasok.

Dengan mengintegrasikan rekomendasi ini ke dalam kerangka kerja ISO/IEC 27001:2022, institusi dapat beralih dari tahap evaluatif menuju tahap implementatif, membangun Information Security Management System (ISMS) yang terukur, terdokumentasi, dan siap diaudit secara internasional.

Tabel 14. Rekapitulasi Hasil Asesmen Indeks KAMI STMIK Palangkaraya

	Skor	Tingkat Kematangan	Arah Peningkatan (ISO/IEC 27001:2022)
Sistem Elektronik	12	I	Penguatan kontrol penggunaan sistem, enkripsi, dan autentikasi pengguna.
Tata Kelola Keamanan Informasi	13	I+	Penetapan kebijakan formal, pembentukan tim keamanan, dan pelatihan SDM.
Pengelolaan Risiko Keamanan Informasi	3	I	Pembentukan kerangka kerja risiko dan penyusunan risk register.
Kerangka Kerja Keamanan Informasi	20	I+	Penguatan dokumentasi, mekanisme evaluasi, dan tinjauan manajemen.
Pengelolaan Aset Informasi	39	II	Inventarisasi, klasifikasi, dan pengendalian akses berbasis peran (RBAC).
Teknologi dan Keamanan Informasi	48	II	Penerapan konfigurasi aman, enkripsi, patch management, dan secure coding.
Pelindungan Data Pribadi (PDP)	31	I+	Pembentukan DPO, kebijakan perlindungan data, dan mekanisme pelaporan insiden.
Suplemen: Pengamanan Keterlibatan Pihak Ketiga	70%	Cukup	Audit dan klausul keamanan dalam kontrak kerja sama pihak ketiga.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil asesmen menggunakan Indeks KAMI versi 5.0, tingkat kesiapan keamanan informasi di STMIK Palangkaraya masih tergolong rendah dengan status "Tidak Layak" terhadap standar ISO/IEC 27001:2022. Sebagian besar domain menunjukkan kelemahan mendasar, terutama pada aspek tata kelola, manajemen risiko, dan kerangka kerja keamanan informasi yang belum terstruktur. Hanya domain pengelolaan aset serta teknologi dan keamanan informasi yang mencapai tingkat kematangan II, namun penerapannya belum konsisten. Aspek perlindungan data pribadi dan pengamanan pihak ketiga telah menunjukkan inisiatif awal, tetapi belum memenuhi standar praktik terbaik.

Untuk mencapai kesesuaian dengan ISO/IEC 27001:2022, institusi perlu menyusun kebijakan formal dan kerangka kerja tata kelola keamanan informasi, membentuk tim dengan peran dan tanggung jawab yang jelas, serta menerapkan manajemen risiko yang sistematis mencakup identifikasi aset, analisis, mitigasi, dan evaluasi berkala. Peningkatan kapasitas teknis melalui penerapan enkripsi, kontrol akses berbasis peran, manajemen log, dan audit aplikasi menjadi prioritas utama. Selain itu, kebijakan perlindungan data pribadi harus diperkuat, termasuk audit kepatuhan dan mekanisme pengawasan terhadap pihak ketiga. Program pelatihan dan kesadaran keamanan informasi yang berkelanjutan perlu diterapkan, disertai asesmen ulang secara periodik untuk memantau efektivitas perbaikan dan mendukung kesiapan menuju sertifikasi ISO/IEC 27001.

DAFTAR PUSTAKA

[1] S. Paramita, S. A. Siregar, R. A. Damanik, and M. D. Irawan, "Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013," *Bulletin of Information Technology (BIT)*, vol. 3, no. 4, pp. 374–379, Dec. 2022, doi: 10.47065/BIT.V3I4.421.

[2] M. P. Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, vol. 13, no. 2, pp. 222–238, Jan. 2023, doi: 10.22212/JP.V13I2.3299.

[3] E. A. Syahnur, M. N. F. Hibrizi, R. Kurnia Lesmana, and M. D. Irawan, "Analisis Manajemen Risiko Keamanan Informasi di PT. Adhi Commuter Properti Medan Menggunakan Standart ISO 31000:2018 (Studi Kasus Hotel Grandhika Medan)," *Balance : Jurnal Akuntansi dan Manajemen*, vol. 1, no. 3, pp. 330–338, Dec. 2022, doi: 10.59086/JAM.V1I3.219.

[4] H. Jauhary, G. E. Pratiwi, A. Z. Salim, and Fitroh, "Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review," *Media Jurnal Informatika*, vol. 14, no. 1, pp. 43–49, Jun. 2022, doi: 10.35194/MJI.V14I1.1581.

[5] T. N. Khusna and B. Sugiantoro, "Pengukuran Tingkat Keamanan Informasi pada UPT-PSI Universitas Muria Kudus berdasarkan Indeks Keamanan Informasi (KAMI) Versi 4.2," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 8, no. 3, pp. 847–856, Aug. 2023, doi: 10.29100/JIPI.V8I3.3720.

[6] Tawar, I. Riadi, A. G. Pratiwi, and A. A. Siregar, "Assessment and Mitigation of Information Security Policy in Budgeting System using KAMI Index 4.1," *Journal of Novel Engineering Science and Technology*, vol. 1, no. 01, pp. 24–29, Aug. 2022, doi: 10.56741/jnest.v1i01.57.

[7] R. Savitri, Firmansyah, Dworo, and M. S. Hasibuan, "Information Security Measurement using INDEX KAMI at Metro City," *Journal of Applied Data Sciences*, vol. 5, no. 1, pp. 33–45, Jan. 2024, doi: 10.47738/JADS.V5I1.152.

[8] R. Dewantara and B. Sugiantoro, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta)," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 8, no. 6, pp. 1137–1148, Nov. 2021, doi: 10.25126/JTIIK.2021863123.

[9] D. I. Khamil, G. M. A. Sasmita, and A. A. N. H. Susila, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 dan ISO/IEC 27001:2013 (Studi Kasus : Diskominfo Kabupaten Gianyar)," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 9, no. 3, pp. 1948–1960, Sep. 2022, doi: 10.35957/JATISI.V9I3.2310.

[10] M. R. balqis S, M. A. Mahadewi, S. A. Imani, and R. Permatasari, "Analisis Kematangan Pengelolaan Keamanan Informasi berbasis Indeks KAMI di PT. BPR Jawa Timur," in *Prosiding Seminar Nasional Teknologi dan Sistem Informasi(SITASI)*, Nov. 2023, pp. 78–86. doi: 10.33005/SITASI.V3I1.546.

[11] A. L. Maryanto, M. N. Al Azam, and A. Nugroho, "Evaluasi Manajemen Keamanan Informasi pada Perusahaan Pemula berbasis Teknologi Menggunakan Indeks KAMI," *Jurnal Simantec*, vol. 11, no. 1, pp. 1–12, Dec. 2022, doi: 10.21107/SIMANTEC.V11I1.14099.

[12] R. Vansuri *et al.*, "Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi," *Jurnal Ilmu Multidisiplin (JIM)*, vol. 2, no. 1, pp. 106–113, Jun. 2023.

[13] M. R. Anwar, D. Apriani, and I. R. Adianita, "View of Hash Algorithm In Verification Of Certificate Data Integrity And Security," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 3, no. 2, pp. 181–188, Sep. 2021, doi: https://doi.org/10.34306/att.v3i2.212.

[14] G. Gafrun and Y. Supit, "Algoritma Tanda Tangan Digital untuk Meningkatkan Keamanan Pesan," *Simtek : jurnal sistem informasi dan teknik komputer*, vol. 9, no. 2, pp. 198–204, Oct. 2024, doi: 10.51876/SIMTEK.V9I2.1294.

[15] K. Chetioui, B. Bah, A. O. Alami, and A. Bahnasse, "Overview of Social Engineering Attacks on Social Networks," *Procedia Comput Sci*, vol. 198, pp. 656–661, Jan. 2022, doi: 10.1016/J.PROCS.2021.12.302.

[16] D. E. Bell, "Bell–La Padula Model," *Encyclopedia of Cryptography, Security and Privacy, Third Edition*, pp. 177–183, Jan. 2025, doi: 10.1007/978-3-030-71522-9_811.

[17] X. Tian and H. Song, "A zero trust method based on BLP and BIBA model," in *Proceedings - 2021 14th International Symposium on Computational Intelligence and Design, ISCID 2021*, Hangzhou, China: Institute of Electrical and Electronics Engineers Inc., Jan. 2022, pp. 96–100. doi: 10.1109/ISCID52796.2021.00031.

[18] F. Haloua, M. Abbas, R. Djerbi, and M. M. Bouhamed, "Formal Modelling and Implementation of Clark-Wilson Security Policy with FoCaLiZe," in *PAIS 2024 - Proceedings: 6th International Conference on Pattern Analysis and Intelligent Systems*, EL OUED, Algeria: Institute of Electrical and Electronics Engineers Inc., Jun. 2024, pp. 1–5. doi: 10.1109/PAIS62114.2024.10541223.

[19] B. Al Faruq, H. R. Herlianto, S. P. H. Simbolon, D. N. Utama, and A. Wibowo, "Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT Services and Security Management System ," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 3514–3531, Jun. 2020.

[20] V. Mahendra and B. Soewito, "Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber," *Techno.COM*, vol. 22, no. 3, pp. 527–538, Aug. 2023.

[21] A. R. S. Wawondatu and Adelia, "Penggabungan Klausul dari Framework ISO/IEC 20000 dan COBIT 5.0 DSS06 dalam Analisis Layanan Teknologi Informasi di Universitas X," *Jurnal*

STRATEGI - Jurnal Maranatha, vol. 2, no. 2, pp. 484–496, Nov. 2020.

[22] T. M. A. Prasetyo and M. N. N. Sitokdana, "Analisis Tata Kelola Pusat Data dan Informasi Kementerian XYZ Menggunakan COBIT 2019," *Journal of Applied Computer Science and Technology*, vol. 2, no. 2, pp. 95–107, Dec. 2021, doi: 10.52158/JACOST.V2I2.265.

[23] muhammad syaiful bahary and B. Sugiantoro, "Evaluasi Tingkat Keamanan Indeks KAMI (Studi Kasus : Universitas X)," *Cyber Security dan Forensik Digital*, vol. 7, no. 2, pp. 90–94, Dec. 2024, doi: 10.14421/csecurity.2024.7.2.4634.

[24] K. Sari, N. Ningsi, N. Zainuddin, and A. M. Sajiah, "Evaluation of Information Security at Benyamin Guluh Kolaka Hospital using the KAMI 4.2 Index with ISO 27001:2013," *Jurnal Media Informasi Teknologi*, vol. 1, no. 1, pp. 23–30, Feb. 2024, doi: 10.69616/MIT.V1I1.161.

[25] Republik Indonesia, *PP No. 71 Tahun 2019*. Indonesia: Pemerintah Pusat, 2019. Accessed: Sep. 09, 2025. [Online]. Available: https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

[26] Republik Indonesia, *UU No. 27 Tahun 2022*. Indonesia: Pemerintah Pusat, 2022. Accessed: Sep. 09, 2025. [Online]. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[27] G. Szyjewski, "Securing digital copies of the documents to ensure documents' integrity," *EUROPEAN RESEARCH STUDIES JOURNAL*, vol. XXVI, no. Issue 4, pp. 718–726, Oct. 2023, doi: 10.35808/ERSJ/3321.

[28] S. Verma, "Information Security Governance: Need of the Hour," in *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-6684-5827-3.ch008*, IGI Global Scientific Publishing, 2022, pp. 110–119. doi: 10.4018/978-1-6684-5827-3.CH008.

[29] M. Sinan, M. Shahin, and I. Gondal, "Implementing and integrating security controls: A practitioners' perspective," *Comput Secur*, vol. 156, p. 104516, Sep. 2025, doi: 10.1016/J.COSE.2025.104516.

[30] A. Z. Mahfud, I. R. Hikmah, S. U. Sunaringtyas, and T. Yulita, "Information Security Risk Management Design Based on ISO/IEC 27005:2022, ISO/IEC 27001:2022, and NIST SP 800-53 Revision 5 (A Case Study at ABC Agency)," in *Proceedings - ICE3IS 2024: 4th International Conference on Electronic and Electrical Engineering and Intelligent System: Leading-Edge Technologies for Sustainable Societies*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 181–186. doi: 10.1109/ICE3IS62977.2024.10775428.

[31] N. Ramadhanty, "Implementasi Kerangka Keamanan NIST Dan ISO/IEC 27001 Dalam Menghadapi Ancaman Risiko Siber," *Journal of Indonesian Management*, vol. 4, no. 4, Nov. 2024, doi: 10.53697/JIM.V4I4.1973.

[32] F. A. Shaikh and M. Siponen, "Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity," *Comput Secur*, vol. 124, p. 102974, Jan. 2023, doi: 10.1016/J.COSE.2022.102974.

[33] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," Apr. 2025. doi: 10.6028/NIST.SP.800-61R3.

[34] M. A. de Carvalho Junior and P. Bandiera-Paiva, "Implications of loosened Role-based Access Control session control implementation for the enforcement of Dynamic Mutually Exclusive Roles properties on Health Information Systems," *Inform Med Unlocked*, vol. 27, p. 100780, Jan. 2021, doi: 10.1016/J.IMU.2021.100780