BAB II

TINJAUAN PUSTAKA

2.1. Keamanan Sistem Informasi

Keamanan sistem informasi menjadi salah satu isu dalam perkembangan teknologi informasi dan komunikasi di era digital (Riadi, 2019). Keamanan informasi merupakan upaya usaha untuk melindungi kerahasiaan, integritas dan ketersediaan data dari berbagai kemungkinan ancaman (Ade Kornelia, 2021). Keamanan informasi menjadi sesuatu yang berharga dimana data yang di terima, di simpan dan di sebarkan menjadi suatu kerahasiaan yang penting yang tidak dapat diketahui oleh orang bebas selain penerima yang dituju oleh kerana itu tata kelola keamanan informasi menjadi sangat penting, karena tata kelola yang baik dapat menjadi acuan untuk melakukan suatu tindakan (Ade Kornelia, 2021) (Pamungkas & Saputra, 2020).

Penerapan keamanan informasi bertujuan untuk mengatasi permasalahan dan hambatan baik teknis maupun non teknis (Riadi, 2019). Keamanan informasi kini telah berkembang menjadi tiga konsep besar, yang dikenal sebagai segitiga CIA, yang telah menjadi standar terdepan dalam industri keamanan (Setyasiwi, 2022):

1. *Confidentiality* (kerahasiaan), yaitu usaha untuk menjaga informasi tetap utuh dan menghindari data dari orang yang tidak memiliki akses. Confidentiality biasanya berupa informasi yang di berikan pada pihak kedua.

2. *Integrity* (integritas), merupakan keaslian dari pesan yang dikirim melakui jaringan, yang menjamin bahwa informasi yang dikirim tidak berubah selama perjalanan.
3. *Availability* (ketersediaan), Kehadiran informasi ketika dibutuhkan disebut sebagai ketersediaan. Serangan / kebocoran sistem informasi dapat menghentikan / meniadakan akses ke data.

Setiap bagian CIA ini sangat penting untuk memastikan sistem informasi aman. Parameter yang digunakan dalam CIA ini menentukan apakah jaringan / informasi dianggap aman. (Jhony Pranata & Nuruzzaman, 2022).

Area keamanan informasi yang baik harus menerapkan standar Deming cycle of quality yang memiliki 4 poin yaitu plan (Merencanakan), Develop (Mengembangkan), Check (Periksa), dan Act (tindakan) (Riadi, 2019).

Keamanan informasi merupakan komponen penting dalam menjaga aset informasi suatu organisasi. Ada beberapa kategori keamanan informasi, seperti yang berikut: (Ade Kornelia, 2021).

1. *Physical security* (keamanan fisik): keamanan yang berfokus pada strategi perlindungan tenaga kerja dan anggota organisasi, aset fisik dan lokasi kerja memiliki banyak bahaya termasuk resiko kebakaran, akses tidak sah, serta bencana alam.
2. *Personal security* (keamanan pribadi): keamanan tumpang tindih dengan keamanan fisik untuk menjamin perlindungan individu dalam bisnis dalam suatu organisasi.

3. *Operational security* (Keamanan Operasional): Keamanan fokus pada strategi untuk memastikan kekuatan perusahaan agar tidak ada hambatan dalam bekerja.
4. *Communications security* (Keamanan Media): Keamanan bertujuan untuk melindungi media, teknologi komunikasi dan kontennya, serta keterampilan yang diperlukan untuk menggunakan alat-alat ini untuk mencapai tujuan perusahaan.
5. *Network security* (Keamanan Siber): Keamanan berfokus pada perlindungan peralatan jaringan, jaringan, dan aset organisasi, serta kemampuan organisasi dalam menggunakan jaringan tersebut untuk menjalankan fungsi komunikasi datanya.

2.2. Manajemen Sistem Keamanan Informasi

Manajemen sistem keamanan informasi (SMKI) ditujukan untuk mencapai tujuan organisasi dengan menetapkan, menerapkan, menggunakan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi (Apriandari & Sasongko, 2018). SMKI penting untuk mengelola informasi dalam suatu perusahaan. Keamanan informasi digunakan untuk menjaga aspek kerahasiaan, integritas, dan ketersediaan informasi (Bakri & Irmayana, 2017). SMKI digunakan untuk meminimalisasi ancaman keamanan informasi. Langkah-langkah dalam perencanaan SMKI meliputi penentuan ruang lingkup, kebijakan, metode penelitian risiko, identifikasi risiko, analisis, penilaian risiko, pilihan manajemen risiko dan pemilihan objek pengendalian (Rahmat, 2019). Keamanan sistem informasi tidak

hanya berkaitan dengan perangkat keras dan perangkat lunak seperti firewall, perangkat lunak anti-virus, penggunaan kata sandi untuk komputer, tetapi juga mengacu pada aspek manusia, proses dan teknologi, di mana menerapkan keamanan untuk menjamin keselamatan selama operasi (Apriandari & Sasongko, 2018). SMKI juga harus mengacu pada standar nasional dan internasional yang ada sehingga kualitas pengamanan yang diberikan lebih baik dan dapat diatasi ketika timbul masalah. Standar internasional yang direkomendasikan untuk penggunaan SMKI adalah ISO/IEC 27001: 2013. Standar ini diterapkan atas dasar risiko sehingga bahaya dapat diminimalkan dan permasalahan tubuh dapat diselesaikan dengan cepat dan akurat (Ade Kornelia, 2021).

Keamanan Informasi (Apriandari & Sasongko, 2018). Manajemen keamanan informasi terdiri dari empat fase, yaitu (Hartati, 2017).

1. Identifikasi ancaman. Serangan terhadap sumber daya informasi suatu bisnis termasuk dalam ancaman keamanan informasi, yaitu organisasi, mekanisme, individu / peristiwa yang berpotensi menyebabkan kejahatan terhadap sumber daya informasi bisnis. Ancaman bisa datang dari dalam maupun luar, baik disengaja maupun tidak disengaja.
2. Identifikasi ancaman dan resiko. Perbuatan tidak sah yang menimbulkan resiko dapat digolongkan menjadi empat kategori:

a. Pencurian dan pengungkapan tidak sah
b. Penggunaan tidak sah
c. Perusakan dan penolakan layanan yang tidak sah
d. Modifikasi (pengubahan / perubahan) yang tidak sah.

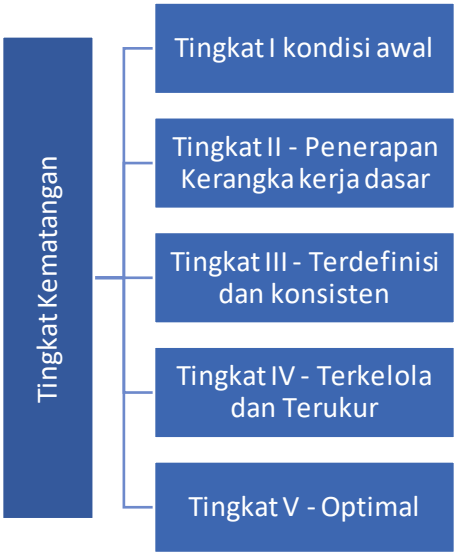
3. Penetapan kebijakan keamanan informasi. Kebijakan keamanan harus diterapkan untuk mengarahkan program secara keseluruhan, terlepas dari apakah perusahaan menggunakan penerapan manajemen risiko / standar emas.
4. Menerapkan pengendalian berbasis resiko. Pengendalian yaitu mekanisme yang diterapkan untuk melindungi bisnis dari risiko / untuk meminimalkan dampak risiko terhadap bisnis.

SMKI penting untuk manajemen informasi dalam bisnis. Keamanan informasi digunakan untuk menjaga aspek kerahasiaan, integritas dan ketersediaan informasi (Ade Kornelia, 2021).

2.3. Index Keamanan Informasi (KAMI)

Indeks Keamanan Informasi (KAMI) yaitu suatu alat bantu penilaian yang melakukan evaluasi tingkat kesiapan (kelengkapan dan kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001 (BSSN, 2021). Penilaian ini bukan acuan untuk analisa kelayakan / efektivitas keamanan yang tersedia, melainkan sebagai alat untuk memberikan gambaran kesiapan kerangka keamanan informasi (Ade Kornelia, 2021) (Husin et al., 2017).

Gambar 2. 1 Area Penilaian Indeks KAMI (BSSN, 2021)



Gambar 2. 2 Tingkat kematangan Indeks KAMI (BSSN, 2021)

Gambar 2.1 dan 2.2 menggambarkan tingkat kematangan ditentukan dengan perhitungian kuesioner, dan setiap bidang terdiri dari lima tingkat yaitu, Level I – Kondisi Awal, Level II – Penerapan Kerangka Dasar, Level III – Pasti dan Konsisten, Level IV – Dapat Dikelola dan Terukur, dan Level V – Optimal

(Pratama et al., 2018). Untuk memberikan gambaran lebih detail, level-level tersebut ditambah dengan level menengah I+, II+, III+, dan IV+ sehingga totalnya ada sembilan level kematangan. Awalnya seluruh Narasumber tergolong pada tingkat kematangan Level I standar ISO 2700: Tahun 2013, dan tingkat kematangan yang diharapkan sebagai standar minimal kesiapan sertifikasi adalah Level III+. (BSSN, 2021).

Evaluasi dapat dilakukan sesuai kebutuhan masing-masing institusi pelaksana. Perwakilan organisasi akan menjawab beberapa pertanyaan yang diajukan dalam indeks KAMI dengan memilih status pelaksanaan, yaitu:

1. Tidak dilaksanakan
2. Belum di terapkan
3. Dilaksanakan sebagian
4. Penerapan di lakukan sesuai standar

2.3.1. 5 Area Evaluasi Indeks KAMI

Evaluasi Indeks KAMI didasarkan pada keseluruhan rentang persyaratan keselamatan yang kini telah direstrukturisasi menjadi lima area. (Wongkar et al., 2015):

1. Tata Kelola - Bagian ini menilai seberapa siap manajemen keamanan informasi, serta institusi, fungsi, dan tanggung jawab pekerja.
2. Manajemen risiko - Bagian ini menilai seberapa siap strategi keamanan informasi untuk menerapkan manajemen risiko keamanan informasi.

3. Kerangka Kerja - Bagian ini menilai kerangka manajemen keamanan informasi (kebijakan dan prosedur) dan metode pelaksanaannya
4. Manajemen Aset Informasi - Bagian ini menilai kecukupan keamanan aset informasi, yang mencakup seluruh siklus hidup aset.
5. Teknologi dan Keamanan Informasi - Bagian ini menilai kelengkapan, konsistensi, dan keberhasilan teknologi yang digunakan untuk mengamankan aset informasi.

2.3.2. Tools Indeks Keamanan Informasi (Indeks KAMI)

Evaluasi dapat dilakukan pada organisasi berukuran besar / kecil. Evaluasi ini sebaiknya dilakukan oleh jabatan yang memegang dan mempunyai tanggung jawab dan wewenang langsung terhadap pengelolaan keamanan informasi.

Proses evaluasi dilakukan melalui pertanyaan di beberapa area berikut (BSSN, 2021):

1. Kategori Sistem Elektronik yang digunakan (Daftar sistem elektronik yang digunakan)
2. Tata Kelola Keamanan Informasi (Manajemen keamanan informasi)
3. Pengelolaan Risiko Keamanan Informasi (Manajemen keamanan informasi)
4. Kerangka Kerja Keamanan Informasi (Kerangka keamanan informasi)
5. Pengelolaan Aset Informasi (Kerangka keamanan informasi)
6. Teknologi dan Keamanan Informasi (Implementasi untuk keamanannya)

7. Suplemen (Langkah-langkah tambahan yang diambil untuk aspek memastikan partisipasi penyedia layanan pihak ketiga, keamanan perlindungan data pribadi dan layanan infrastruktur cloud).

Apabila alat evaluasi ini digunakan dengan prinsip kejujuran dan keterbukaan, hasilnya akan menguntungkan semua pihak. Pertanyaan dikategorikan dengan dua alasan. Pertama, pertanyaan diklasifikasikan menurut tingkat kesiapan implementasi keamanan dengan kriteria kelengkapan kontrol yang disyaratkan oleh standar ISO/IEC 27001:2013. Narasumber diminta untuk memberikan informasi tentang berbagai aspek kerangka keamanan informasi, mulai dari sifat dasar kerangka tersebut (pertanyaan diberi label "1"), efektivitas dan konsistensi penerapan (pertanyaan diberi label "2"), dan kemampuan untuk terus meningkatkan kinerja keamanan informasi (pertanyaan diberi label "3"). tingkat persiapan minimum yang diperlukan untuk proses sertifikasi ISO/IEC 27001:2013.

Setiap jawaban diberikan skor/nilai yang akan dikonsolidasi untuk menghasilkan angka.

Tabel 2. 1 Nilai Skor Penggunaan Indeks KAMI (BSSN, 2021)

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

Ketentuan nilai:

1. Bila kategori pengamanan 1 maka diberi nilai 0, 1, 2 dan 3
2. Bila kategori pengamanan 2 maka diberi nilai 0, 2, 4 dan 6
3. Bila kategori pengamanan 3 maka diberi nilai 0, 3, 6 dan 9

Terlihat pada table 2.1 pada nilai skor ini akan menggabungkan penilaian dari bertanyaan sebelumnya untuk semua area pengamanan, pengisian pertanyaan dengan label "3" hanya dapat menghasilkan nilai apabila semua pertanyaan yang terkait dengan label "1" dan "2" sudah diisi dengan status minimal "Diterapkan Sebagian". Apabila nilai yang di terapkan pada label "1" dan "2" diisi "Tidak Dilakukan" / "Dalam Perencanaan", maka hasil selanjutnya akan menghasilkan nilai "0" walaupun status penerapannya "Diterapkan secara Menyeluruh".

Radar tersebut memiliki zona dasar tingkat kematangan maksimum dari 1 hingga 3. Pada diagram ini terlihat perbandingan antara tingkat kesiapan yang diperoleh dari penilaian dengan tingkat kematangan yang ada. Membaca diagram

ini mengungkapkan perlunya perbaikan dan keterkaitan antara berbagai bidang penerapan keamanan informasi.

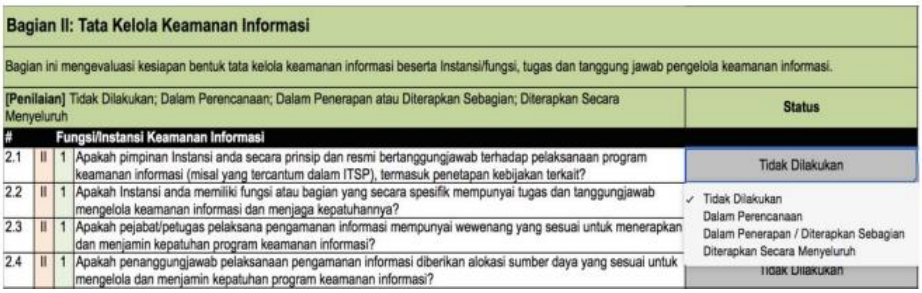
Korelasi kategori sistem elektronik (ES) dengan tingkat kesiapan dapat dilihat pada Tabel 2.4:

KATEGORI SISTEM ELEKTRONIK				
Rendah		**Skor Akhir**		**Status Kesiapan**
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

Gambar 2. 3 Nilai Kategori Sistem Elektronik (BSSN, 2021)

Pengelompokan kedua didasarkan pada tingkat kematangan implementasi keamanan, dan klasifikasi mengacu pada tingkat kematangan yang digunakan dalam kerangka COBIT / CMMI. Tingkat kematangan ini digunakan sebagai alat pelaporan untuk memetakan dan mengurutkan kesiapan keamanan informasi antar departemen/lembaga. Pertama, seluruh Narasumber masuk dalam tingkat kematangan I yang sesuai dengan standar ISO 2700. Tingkat kematangan minimum yang diharapkan untuk persiapan sertifikasi adalah Level III+.

Gambar di bawah menunjukkan label kematangan (kolom di sebelah kanan nomor) dan kelengkapan (kolom di sebelah kiri pertanyaan) terlihat pada gambar 2.5.



Bagian II: Tata Kelola Keamanan Informasi

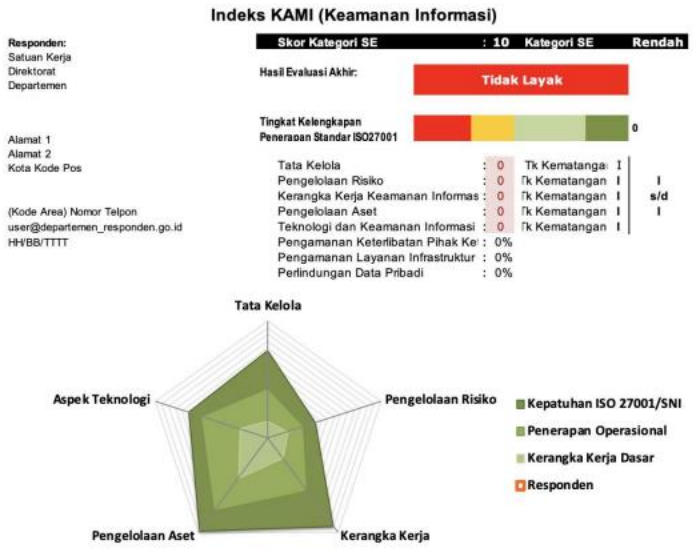
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status
#			Fungsi/Instansi Keamanan Informasi	
2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Tidak Dilakukan
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	✓ Tidak Dilakukan Dalam Perencanaan Dalam Penerapan / Diterapkan Sebagian Diterapkan Secara Menyeluruh
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan

Gambar 2.4 Label Pengelompokan Kematangan (BSSN, 2021)

Kedua pengelompokan ini Tersedia dua tampilan yang berbeda: Tingkat Penerimaan Keamanan dan Tingkat Kematangan Keamanan. Organisasi yang merespons dapat menggunakan indikator ini untuk menginformasikan inisiatif keamanan informasi terlihat pada gambar 2.5 dan 2.6.

Gambar 2.5 Nilai Rentang Kelengkapan Pengamanan (BSSN, 2021)



Gambar 2. 6 Dashboard Indeks KAMI (BSSN, 2021)

Gambar 2.7 *Dashboard* dari Indeks KAMI yang merupakan gambaran yang didapat dari alat evaluasi Indeks KAMI yang dilakukan pada institusi, indeks KAMI memuat nilai total setiap area dan mencerminkan nilai total disajikan dalam diagram batang dan radar untuk menunjukkan kematangan keamanan data.

2.4. ISO/IEC 27001:2013

ISO 27001 adalah suatu standar global untuk sistem manajemen keamanan informasi (Hartati, 2017). SNI ISO/IEC 27001 dibuat berdasarkan kebutuhan, tujuan, dan persyaratan keamanan organisasi, menjadikannya standar internasional yang *fleksibel*, menurut Sarno dan Iffano (2009) (Rahmat, 2019). Selain itu, SNI ISO/IEC 27001 memberikan sertifikat penerapan SMKI yang diakui secara nasional dan internasional disebut *Information Security Management System* (ISMS) (Rahmat, 2019). ISO 27001 berlaku untuk semua industri. Keamanan

informasi yang disimpan dalam bentuk apapun, tidak hanya ber1upa data elektronik (Hartati, 2017).

Standar Nasional Indonesia (SNI) ISO/IEC 27001:2013 merupakan standardisasi dalam lingkup Sistem Manajemen Keamanan Informasi (SMKI) (Apriandari & Sasongko, 2018). Standar tersebut dirancang secara khusus untuk mempersiapkan persyaratan pembentukan, penerapan, pemeliharaan dan perbaikan berkelanjutan suatu SMKI (Ade Kornelia, 2021). intinya, suatu lembaga dapat memilih standar mana yang akan digunakan untuk mendukung SMKI, salah satunya adalah dengan mengadopsi standar dari *International Organization for Standardization* (ISO) atau *International Electrotechnical Commission* (IEC) 27001: 2013 dengan karakteristik pengendalian tertentu. Perancangan SMKI pada penelitian ini mengacu pada standar SNI ISO/IEC 27001:2013, dengan menggunakan dokumen kebijakan tingkat 1, penilaian risiko, pelingkup dan pernyataan implementasi (*Statement Of Applicability* (SOA) dan dokumen tingkat 2 yang menunjukkan prosedur keamanan informasi (Rahmat, 2019).

Manfaat ISO 27001, antara lain (Ade Kornelia, 2021):

1. Memberikan kepercayaan dan kepastian kepada pelanggan dan hubungan bisnis jika perusahaan telah memiliki SMKI yang baik sesuai standar internasional. Selain itu, ISO 27001 juga dapat digunakan dalam pemasaran bisnis.
2. Pastikan organisasi memiliki kendali terkait keamanan informasi di lingkungan proses bisnis yang dapat menimbulkan bahaya / hambatan.

3. ISO 27001 mengharuskan untuk selalu memperkuat keamanan informasi perusahaan. Hal ini membantu menentukan lebih lanjut tingkat keamanan yang sesuai yang dibutuhkan bisnis. Sumber daya yang digunakan disesuaikan dengan kebutuhannya.

Struktur organisasi ISO/IEC 27001:2013 dibagi menjadi bagian, diantaranya (Apriandari & Sasongko, 2018).

1. *Klausul*: prosedur yang mewajibkan jika organisasi menetapkan SMKI, klausul (pasal) persyaratan harus dipenuhi saat menggunakan SNI ISO/IEC 27001:2013
2. *Annex* (lampiran) A: Lampiran kontrol keamanan yaitu dokumen yang disediakan yang dapat digunakan untuk menentukan kontrol keamanan yang harus diterapkan di SMKI. Terdapat 14 klausul pengendalian keamanan, 35 tujuan manajemen, dan 114 pengendalian keamanan informasi.

Area yang digunakan dalam indeks KAMI untuk menilai / mengukur kematangan SMKI suatu lembaga merangkum empat belas tujuan pengelolaan ISO 27001: 2013 menjadi lima area penilaian. (Dewantara & Sugiantoro, 2021).

2.5.Penelitian Terkait (*State-Of-The-Art*)

Berikut ini tabel penelitian *State-Of-The-Art* dapat dilihat pada tabel 2.2

Tabel 2. 2 Perbandingan Hasil Penelitian Terkait

Penelitian Terkait Analisis Indeks Keamanan Informasi 4.2			
No	Penulis dan Tahun Penelitian	Judul Penelitian	Hasil Penelitian
1	Dicky Insan Khamil, Gusti Made Arya Sasmita, Anak Agung Ngurah Hary Susila/2022 (Khamil, 2022)	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)	Kesimpulan persentase Tingkat Kematangan Tertinggi berada Teknologi dan keamanan informasi, dan setidaknya beberapa bidang merupakan bidang yang saling melengkapi.Hasil Evaluasi mendapatkan skor akhir pada Kategori Sistem Elektronik sebesar 34 yang termasuk dalam kategori "Tinggi", dan skor akhir Kategori Keamanan Informasi sebesar 190.
2	I Putu Setyo Syahindra, Clara Hetty Primasari, Aloysius Bagas Pradipta Irianto/2022	Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks Kami Dan Iso 27005: 2011	Tingkat kelengkapan sebesar 457 yang sudah termasuk "Cukup Baik" pada pemenuhan standar ISO/IEC 27001. tapi tingkat kematangan secara keseluruhan baru menyentuh pada III+ artinya hasil penilaian belum sesuai dengan ISO/IEC 27001.
3	Ade Kornelia & Dedi Irawan/ 2021 (Ade Kornelia, 2021)	Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1	Hasil pengujian kerentanan sistem menggunakan OWASP Zap tool menunjukkan 4 kerentanan yang perlu diperbaiki: A01 - Kontrol akses rusak, A05 - Kesalahan konfigurasi keamanan, A08 - Hilangnya integritas data dan perangkat lunak, dan A09 - Kesalahan pencatatan dan pemantauan keamanan.
4	Rizki Dewantara, Bambang Sugiantoro/2021 (Dewantara & Sugiantoro, 2021)	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Jaringan (Studi Kasus: Uin Sunan Kalijaga Yogyakarta)	Menunjukkan peningkatan skor evaluasi sebesar 25, setelah sebelumnya menerapkan OSSIM tanpa menerapkan OSSIM dengan skor dari 407 menjadi 432.
5	Gede Dandy Salodivansa Barani / 2020 (Dandy et al., 2020)	Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI (Keamanan Informasi) 4.0 (Studi Kasus: Dinas Komunikasi Dan Informatika Provinsi Jawa Timur)	Hasil analisis tersebut menjadi dasar rekomendasi berdasarkan pengendalian ISO27001, salah satu rekomendasi terkait strategi keamanan informasi berdasarkan pengendalian A.5.1.1
6	Desy Dwi Prasetyowati / 2019 (Prasetyowati et al., 2019)	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 Pada Politeknik Ilmu Pelayaran Semarang	Hasilnya adalah skor 20 yang diciptakan oleh sistem elektronik dan tingkat keandalan informasi sebesar 238. Oleh karena itu, PIP memerlukan perubahan dan perbaikan pada sistem yang ada saat

Penelitian Terkait Analisis Indeks Keamanan Informasi 4.2			
No	Penulis dan Tahun Penelitian	Judul Penelitian	Hasil Penelitian
			ini, serta staf yang aktif menangani permasalahan tersebut.
7	Edo Rizky Pratama/ 2018 (Pratama et al., 2018)	Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI Dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur)	Hasil analisis menunjukkan bahwa beberapa tindakan pengendalian ISO 27001: 2013 tidak terpenuhi berdasarkan area indeks KAMI masing-masing. Pengendalian yang tidak patuh ini akan menjadi acuan dalam pembuatan rekomendasi.
8	Ferdian Satria Sujalma, Awalludiyah Ambarwati, Natalia Damastuti/ 2017 (Sujalma et al., 2017)	Evaluasi Keamanan Informasi Pada Pt. Ma-Ri Menggunakan Indeks Kami	Hasil penggunaan memperoleh 17 poin (dari 50) untuk tingkat kinerja dan keunggulan di bidang ICT (Teknologi Informasi dan Komunikasi). Mari sangat tinggi. Hasil asesmen pada lima area yaitu 249 dari 588 berada pada level I-I+ tahap awal pada penerapan keamanan informasi.
9	Astri F. Manullang, Candiwan, Listyo Dwi Harsono3 (Manullang et al., 2017)	Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) pada Institusi Xyz	Hasil menunjukkan tingkat ketergantungan terhadap Sistem Elektronik yang tinggi tetapi status kesiapan dalam manajemen keamanan informasi tidak layak dan berada pada level I-I+ yang berada pada kondisi awal penerapan keamanan informasi
10	Muh. Faturachman Husin / 2017 (Husin et al., 2017)	Implementasi Indeks KAMI Di Universitas Sam Ratulangi	Skor akhir Indeks KAMI yaitu 191 dari 588 skor maksimum / 32.48%. Dengan skor ini, yang hasilnya belum sesuai dengan standar keamnana yang baik.

2.6. Matriks Penelitian

Berikut ini tabel matriks penelitian yang dapat dilihat pada tabel 2.3 sampai 2.4

Tabel 2. 3 Matriks Penelitian

No	Penulis/tahun	Judul Penelitian	Ruang Lingkup Penelitian		
			ISO/IEC 27001/2013	Audit	Indeks KAMI
1	Eko Jhony Pranata / 2022 (Jhony Pranata & Nuruzzaman, 2022)	Optimasi Keamanan Informasi Menggunakan Manajemen Indeks Keamanan Informasi (Kami) Studi Kasus: Ibisa Purworejo	✗	✓	✓
2	Dicky Insan Khamil/2022 (Khamil, 2022)	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)	✓	✓	✓
3	I Putu Setyo Syahindra, Clara Hetty Primasari, Aloysius Bagas Pradipta Irianto/2022	Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks Kami Dan Iso 27005: 2011	✓	✓	✓
4	Ade Kornelia & Dedi Irawan (Ade Kornelia, 2021)	Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1	✓	✓	4.1
5	Rizki Dewantara, Bambang Sugiantoro (Dewantara & Sugiantoro, 2021)	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Jaringan (Studi Kasus: Uin Sunan Kalijaga Yogyakarta)	✗	✓	✓

Tabel 2. 4 Matriks Penelitian (Lanjutan 1)

No	Penulis/tahun	Judul Penelitian	Ruang Lingkup Penelitian		
			ISO/IEC 27001/2013	Audit	Indeks KAMI
6	Gede Dandy Salodivansa Barani (Dandy et al., 2020)	Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI (Keamanan Informasi) 4.0 (Studi Kasus: Dinas Komunikasi Dan Informatika Provinsi Jawa Timur)	✗	✓	0.4
7	Desy Dwi Prasetyowati (Prasetyowati et al., 2019)	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 Pada Politeknik Ilmu Pelayaran Semarang	✓	✓	3.1
8	Ferdian Satria Sujalma (Sujalma et al., 2017)	Evaluasi Keamanan Informasi Pada PT. Ma-Ri Menggunakan Indeks KAMI	✗	✓	✓
9	Muh. Faturachman Husin (Husin et al., 2017)	Implementasi Indeks KAMI Di Universitas Sam Ratulangi	✗	✓	✓
10	Astri F. Manullang1, Candiwan, Listyo Dwi Harsono (Manullang et al., 2017)	Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) pada Institusi Xyz	✗	✓	✓
11	Mega Senlian Jenny	Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks Kami) Versi 4.2 Pada Sistem Informasi Akademik (Simak) Universitas Siliwangi	✓	✓	4.2

Penelitian yang dilakukan menggunakan indeks KAMI versi 4.2 untuk menganalisis kesiapan keamanan informasi pada SIMAK UNSIL, dan memberikan gambaran kondisi kesiapan keamanan informasi berdasarkan hasil program kerja yang dilakukan, serta sarana menyampaikan peningkatan kesiapan keamanan informasi yang dilakukan kepada UPA TIK penelitian ini bertujuan untuk melihat keamanan informasi yang di terapkan apakah sudah memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013. Penelitian ini akan memberikan hasil dari kuesioner berupa skor yang di gunakan pada indeks KAMI 4.2, hasil akhir akan berupa gambaran juga penjelasan atas perbandingan skor indeks KAMI dan ISO 27001/2013 dan penelitian ini akan memberikan rekomendasi sebagai bahan pertimbangan perbaikan untuk kesiapan keamanan informasinya.