BAB II
EVALUASI TINGKAT KESIAPAN KEAMANAN INFORMASI

2.1. Dasar Teori

2.1.1. Keamanan Informasi

Keamanan informasi merupakan upaya untuk melindungi aset informasi dari ancaman yang muncul [9]. Keamanan informasi mencakup perlindungan pada aspek-aspek berikut [9]:

1. *Confidentiality* (kerahasiaan), Adalah aspek yang berfungsi untuk memastikan kerahasiaan data atau informasi, membuatn data hanya dapat diakses oleh orang yang berwenang, dan memastikan kerahasiaan data yang dikirim, diterima, dan disimpan.
2. *Integrity* (integritas), Merupakan aspek yang mencegah data diubah tanpa izin dari otoritas yang berwenang, dan merupakan metode untuk menjaga integritas informasi dan memastikan aspek integritas.
3. *Availability* (ketersediaan), Ini adalah aspek yang berfungsi untuk memastikan bahwa data tersedia saat dibutuhkan dan bahwa informasi dan alat yang relevan dapat diakses oleh pengguna.

Karena pentingnya penerapan keamanan informasi untuk melindungi aset informasi, maka diperlukan manajemen risiko yang berfungsi mengamankan aset informasi. Penerapan pengendalian yang konsisten dengan prosedur yang ditetapkan untuk upaya keamanan informasi merupakan faktor yang dapat membantu mengurangi risiko yang mungkin terjadi.

Keamanan informasi merupakan bagian integral dari suatu sistem yang dibentuk berdasarkan risiko bisnis, pengembangan, implementasi, operasi, pemantauan dan pemeliharaan, kerangka keamanan informasi harus didukung oleh aspek-aspek berikut [10].

1. Struktur organisasi, berupa fungsi atau jabatan yang berkaitan dengan keamanan informasi
2. Kebijakan keamanan, berupa peraturan dasar tentang penanganan insiden, akses dan pengelolaan yang berkaitan dengan keamanan informasi
3. Prosedur dan proses, berupa prosedur yang berkaitan dengan pengimplementasian keamanan informasi.
4. Tanggung jawab, berupa konsep dan aspek keamanan informasi dalam deskripsi pekerjaan pada setiap jabatan dalam perusahaan.

2.1.2. **Kesiapan Keamanan Informasi**

Kesiapan keamanan informasi yang terstruktur merupakan hal yang menjadi kebutuhan dalam setiap penyelenggara layanan publik yang berbasis pada internet dan intranet baik secara *offline* maupun *online* [11]. Perlunya keamanan informasi yang terstruktur untuk mencegah terjadinya pencurian data dari pihak yang tidak berwenang. Oleh karena itu, maka perlunya dilakukan audit terhadap keamanan informasi secara berkala

Salah satu standar yang digunakan untuk melakukan audit terhadap keamanan informasi adalah ISO 27001. *International Standard Organization* (ISO) merupakan salah satu standar yang dapat diterapkan secara internasional dengan alasan pentingnya sebuah standarisasi dalam bidang industri. ISO 27001 merupakan salah satu penerapan standar dalam bidang manajemen keamanan informasi [12].

ISO 27001 merupakan standar yang digunakan untuk mengetahui kebutuhan penerapan keamanan sistem informasi dalam melindungi aspek keamanan informasi yang terdiri dari *confidentiality*, *integrity*, dan *availability* [13]. ISO 27001 merupakan standar keamanan informasi yang berisikan spesifikasi yang harus dipenuhi saat membangun Sistem Manajemen Keamanan Informasi (SMKI) dengan tujuan untuk menjamin keamanan yang melindungi aset informasi dari risiko.

ISO 27001 berisikan aspek pendukung untuk terjadinya realisasi dan implementasi sistem manajemen keamanan informasi dalam perusahaan yang terdiri 11 aspek, yaitu [14]:

1. *Security policy*
2. *Organization of information security*
3. *Asset management*
4. *Human resource security*
5. *Physical and environmental security*
6. *Communication and operations management*
7. *Access control*
8. *Information system acquisition, development, and maintenance.*
9. *Information security incident management.*
10. *Business continuity management.*
11. *Compliance.*

Aspek tersebut diharapkan dapat memberi keyakinan untuk melindungi informasi dan mengelola keamanan informasi dengan tujuan mencapai kepatuhan pada keamanan informasi.

Kelebihan dari ISO 27001 adalah memberikan gambaran secara umum tentang kebutuhan dalam perusahaan/organisasi untuk mengimplementasikan keamanan informasi dan disesuaikan dengan tujuan, sasaran dan kebutuhan dalam perusahaan/organisasi [15].

Standar lainnya yang digunakan adalah COBIT. Standar *Control for Information and Related Technology* (COBIT) merupakan standar yang memberikan kerangka dasar untuk menciptakan teknologi informasi sesuai dengan kebutuhan organisasi. COBIT menyediakan solusi tata kelola teknologi informasi melalui *domain*, proses, tujuan, kegiatan, model kematangan, dan struktur yang teratur [16]. Kelebihan dari COBIT adalah cakupannya yang meliputi keseluruhan dalam tata kelola teknologi informasi dikarenakan COBIT bergerak sebagai integrator dari

implementasi IT *governance* yang juga melibatkan petinggi manajemen dalam pertimbangannya.

2.1.3. **Indeks KAMI versi 4.1**

Indeks Keamanan Informasi (KAMI) versi 4.1 merupakan metode untuk menganalisis dan mengevaluasi integritas dan maturitas aplikasi keamanan informasi sesuai standar SNI ISO/IEC 27007 yang terdiri dari tata kelola, manajemen risiko, kerangka kerja, manajemen aset, dan aspek teknis yang dilakukan oleh pejabat/staff yang memiliki wewenang dalam lingkungan organisasinya [17].

Indeks Keamanan Informasi (KAMI) versi 4.1 merupakan perangkat untuk melakukan analisis dan evaluasi tingkat kesiapan (kelengkapan dan kematangan) keamanan informasi dalam lembaga pemerintah menurut kriteria SNI ISO/IEC 27001 [18].

Penilaian Indikator Indeks KAMI versi 4.1 dirancang dan dapat diterapkan pada organisasi dengan tingkat, ukuran dan tingkat kepentingan yang berbeda dalam menggunakan TIK untuk mendukung pelaksanaan proses yang ada [19]. Indeks KAMI versi 4.1 dapat digunakan secara berkala untuk lebih memahami perubahan kondisi keamanan informasi.

Proses evaluasi dilakukan sesuai dengan panduan pada Indeks KAMI versi 4.1 [20]. Pertanyaan yang digunakan untuk proses evaluasi adalah:

1. Tata Kelola Keamanan Informasi
2. Pengelolaan Risiko Keamanan Informasi
3. Kerangka Kerja Keamanan Informasi
4. Pengelolaan Aset Informasi
5. Teknologi dan Keamanan Informasi
6. Suplemen

Pada tahap awal, responden harus menentukan jenis sistem elektronik dalam organisasi. Responden juga diminta untuk menjelaskan secara singkat infrastruktur TIK di unit kerjanya. Tujuan dari proses ini adalah untuk mengklasifikasikan sistem elektronik yang digunakan oleh instansi pemerintah ke dalam "tingkat" tertentu (rendah, tinggi, strategis) sehingga pemetaan dapat dilakukan lintas instansi dengan karakteristik yang sama titik sistem elektronik. Berikut adalah contoh bagaimana kategori Sistem Elektronik ditampilkan pada Indeks KAMI versi 4.1 pada Tabel 2.2

Tabel 2. 1 Contoh Kategorisasi Sistem Elektronik pada Indek KAMI versi 4.1

Bagian I: Kategori Sistem Elektronik		
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan		
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**
#	**Karakteristik Instansi/Perusahaan**	
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	C
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	B

Berdasarkan Tabel 2.1 di atas, masing-masing fitur memiliki status evaluasi A, B dan C dengan nilai pembobotannya masing-masing. A memiliki nilai pembobotan 5, B memiliki nilai pembobotan 2 dan C memiliki nilai pembobotan 1. Sehingga akan memperoleh tingkat ketergantungan suatu instansi terhadap sistem elektronik.

Masing-masing area dalam Indeks KAMI bersi 4.1, berisikan penilaian yang memuat tentang hal yang berguna demi tercapainya tujuan untuk setiap aspek pengamanan pada Indeks KAMI versi 4.1 dan juga agar dapat dilakukam sertifikasi

berdasarlkan standar SNI ISO/IEC 27001:2011. Tabe; 2.2 merupakan contoh pertanyaan pada aspek pengelolaan risiko dalam Indeks KAMI versi 4.1

Tabel 2. 2 Contoh pertanyaan aspek pengelolaan risiko keamanan informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi				
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Kajian Risiko Keamanan Informasi**	
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Dalam Perencanaan

Pertanyaan Indeks KAMI versi 4.1 berdasarkan pada kesediaan untuk menerapkan tindakan perlindungan sesuai dengan kelengkapan tindakan pengendalian yang dipersyaratkan oleh ISO/IEC 27001: 2013. Responden diminta untuk memberikan jawaban dari bidang yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (pertanyaan berlabel "1"), efektivitas dan konsistensi aplikasi (label "2"), kemampuan untuk terus meningkatkan kinerja keamanan informasi (label "3").

Setiap pemilihan jawaban memiliki bobot nilainya masing-masing, berikut gambat 2.1 yang merupakan pemetaan skor untuk penilaian Status Penerapan instansi yang digunakan pada pertanyaan di seluruh bagian atau aspek.

Tabel 2. 3 Matriks Bobot Penilaian Status Penerapan

	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

Tabel 2.3 berikut merupakan pemetaan dari skor penilaian status penerapan pada instansi dari setiap pertanyaan dalam seluruh area. Jumlah pertanyaan dalam area ditetapkan berdasarkan tingkat kematangan dan pengamanan yang akan dijelaskan pada Tabel 2.4 berikut.

Tabel 2. 4 Jumlah Pertanyaan Berdasarkan Tingkat Kematangan dan Pengamanan

Tingkat Kematangan	Kategori Pengamanan	Area Evaluasi				
		Tata Kelaola	Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
I	-	-	-	-	-	-
II	1	8	10	9	24	14
	2	5	-	2	5	-
III	1	-	-	3	-	-
	2	3	2	8	5	10
	3	-	-	2	4	1
IV	2	-	2	-	-	-
	3	6	-	3	-	1
V	3	-	2	2	-	-

Tabel 2.3 dan 2.4 menunjukan jumlah pertanyaan pada seluruh area evaluasi yang berdasar pada Kategori Pengamanan yang didapatkan dari responden. Hubungan

antara Kategori Sistem Elektronik dengan Status Kesiapan dijelaskan melalui Tabel 2,5 berikut.

Tabel 2. 5 Detail Tingkat Ketergantungan pada Kategori Sistem Elektronik

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

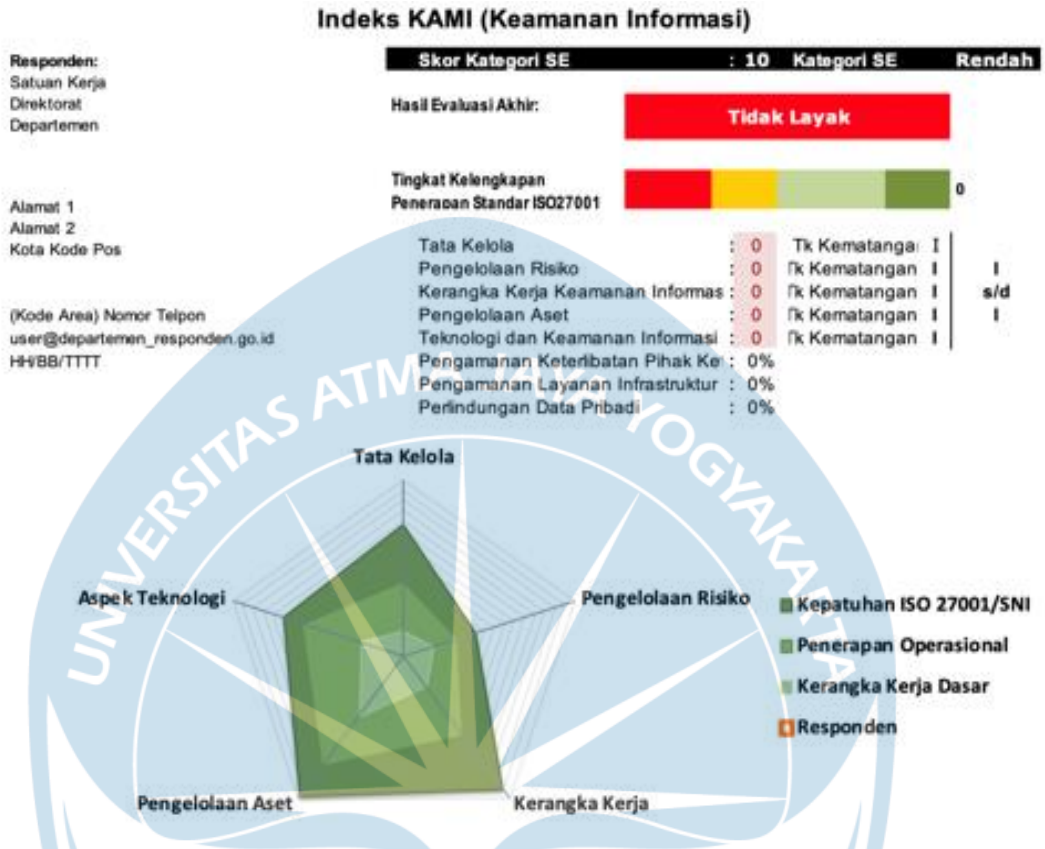
Persyaratan kedua didasarkan pada tingkat kematangan aplikasi keamanan. Untuk Indeks KAMI versi 4.1, tingkat kematangan didefinisikan sebagai berikut:

- Tingkat I - Kondisi awal
- Tingkat II - Penerapan Kerangka Kerja Dasar
- Tingkat III - Terdefinisi dan konsisten
- Tingkat IV - Terkelola dan Terukur
- Tingkat V - Optimal.

Untuk penjelasan yang lebih rinci maka ditambahkan + dan – sehingga tingkat kematangan ada 9 tingkat yaitu I, I+, II, II+, III, III+, IV, IV+, dan V. Berikut gambar 2.3 akan menggambarkan rentang kelengkapan pengamanan.

Gambar 2. 1 Rentang Tingkat Kematangan

Berdasarkan Gambar 2.1 di atas, Level III+ merupakan minimal yang harus dicapai untuk dapat dikatakan layak. Batas minimal tersebut sesuai dengan ISO 27001, sehingga instansi dengan hasil penilaian di bawah batas minimal dianggap tidak sesuai dan harus meningkatkan kesiapan keamanan informasinya. Gambar 2.2 adalah contoh bagaimana menampilkan lembar hasil penilaian menggunakan Indeks KAMI versi 4.1.



Gambar 2. 2 Contoh Tampilan Lembar Hasil Penilaian Menggunakan Indeks KAMI versi 4.1

2.1.4. **Pengelolaan Risiko Keamanan Informasi**

Pengelolaan risiko keamanan informasi merupakan metode penilaian dan mitigasi risiko terhadap aspek utama dalam keamanan informasi yang berisikan 3 unsur penting, yaitu: *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) [21]. Berdasarkan pada Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 7 tahun 2018 [8], manajemen risiko keamanan informasi merupakan salah satu syarat Penyelenggaran Sistem Elektronik (PSE).

Risiko keamanan informasi merupakan bagian dari risiko operasional dikarenakan penggunaan aset teknologi informasi yang mendukung berjalannya proses operasional dan proses bisnis dalam perusahaan [22]. Oleh karena itu, penting untuk mempraktikkan keamanan informasi untuk mencegah segala upaya untuk

mencuri atau menghancurkan informasi di dalam atau di luar organisasi. Upaya yang dapat dilakukan untuk meningkatkan keamanan informasi adalah dengan merencanakan, mengembangkan dan memantau berbagai kegiatan terkait informasi dan data ditulis sesuai fungsinya dan tidak boleh disalahgunakan oleh pihak yang tidak berwenang [10].

Standar lainnya yg sanggup dipakai menjadi panduan pengukuran pengelolaan risiko keamanan informasi pada antaranya COBIT (*Control Objective for Information and related Technology*), FMEA (*Failure Model Effect Analysis*) & lainnya. Metode COBIT digunakan oleh Dewi Ciptaningrum, Eko Nugroho, & Dani Adipta untk melakukan audit keamanan sistem informasi dalam tempat kerja pemerintahan Kota Yogyakarta [10]. Sedangkan metode FMEA dipakai dalam penelitian pada Universitas Dian Nuswantoro dengan tujuan mitigasi risiko aset & komponen teknologi informasi yang dilakukan oleh Gunawan Setyiadi & Yupie Kusumawati [23].

2.1.5. **ISO/IEC 27001:2013**

ISO/IEC 27001:2013 adalah panduan pembuatan dan penggunaan langkah-langkah untuk mengevaluasi efektivitas penerapan SMKI sesuai dengan ISO/IEC 27001, termasuk langkah-langkah berikut [20].

- Penjelasan tentang pengukuran keamanan informasi
- Tanggung jawab manajemen
- Pengembangan metode pengukuran
- Pengukuran operasi
- Analisis data dan pelaporan hasil pengukuran
- Evaluasi dan perbaikan program pengukuran keamanan informasi

ISO/IEC 27001:2013 merupakan standar manajemen keamanan internasional yang menentukan praktik manajemen keamanan yang komprehensif sesuai dengan panduan praktik terbaik ISO/IEC 27001 [15]. ISO/IEC 27001:2013 memiliki sifat

independen terhadap teknologi informasi sehingga pendekatan yang dilakukan berbasis risiko dan bertujuan untuk memastikan kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko [24].

ISO/IEC 27001:2013 berisikan 14 klausul yang mencakup 113 kontrol didalamnya [30]. Berikut merupakan klausul dalam ISO/IEC 27001:2013 [25]:

1. *A.5: Information security policies*
2. *A.6: How information security is organized*
3. *A.7: Human resources security – controls that are applied before, during, or after employment.*
4. *A.8: Asset management*
5. *A.9: Access controls and managing user access*
6. *A.10: Cryptographic technology*
7. *A.11: Physical security of the organization's sites and equipment*
8. *A.12: Operational security*
9. *A.13: Secure communications and data transfer*
10. *A.14: Secure acquisition, development, and support of information systems*
11. *A.15: Security for suppliers and third parties*
12. *A.16: Incident management*
13. *A.17: Business continuity/disaster recovery (to the extent that it affects information security)*
14. *A.18: Compliance – with internal requirements, such as policies, and with external requirements, such as laws.*

Dalam pelaksanaannya, pihak instansi atau perusahaan dapat memilih kontrol yang paling relevan dengan kondisi dalam perusahaan sesuai dengan penilaian yang sudah dilakukan terhadap risiko dan aset pada tahapan awal [25].

2.2. Studi Sebelumnya

Penelitian sebelumnya yang dilakukan oleh I Putu Setyo Syahindra pada tahun 2022 melakukan evaluasi risiko keamanan informasi menggunakan indeks KAMI yang dilakukan oleh Dinas Komunikasi dan Informasi Provinsi XYZ [2]. Tujuan dari penelitian ini adalah menggunakan Indeks KAMI untuk mengevaluasi risiko keamanan informasi di Dinas Komunikasi dan Informasi Provinsi XYZ. Hasil penelitian ini mengajukan saran dan menjadi acuan untuk meningkatkan tingkat keamanan informasi di Dinas Komunikasi dan Informasi Provinsi XYZ.

Penelitian ini dilakukan dengan terlebih dahulu menelusuri sumber-sumber perpustakaan, kemudian memahami standar yang digunakan, kemudian mengumpulkan data yang diperoleh dengan kuesioner dan wawancara tidak terstruktur, dan mengevaluasi studi kasus sesuai standar ISO 27001. Rekomendasi diberikan pada bagian pengelolaan risiko keamanan informasi.

Hasil dari penelitian ini menunjukan jika Diskominfo Provinsi XYZ memiliki ketergantungan yang tinggi untuk penggunaan sistem elektronik dalam berjalannya proses bisnis instansi dengan tingkat kelengkapan sebesar 457 dan sudah masuk kedalam katogori “Cukup Baik” berdasarkan standar ISO/IEC 27001. Untuk tingkat kematangan menyelutuh baru mencapai III+ yang bisa terbilang baru menyetuh standar minimal menurut standar ISO 27001/SNI. Pada area pengelolaan risiko keamanan informasi, persentase yang didapatkan berada pada tingkat rendah sehingga belum memenuhi tingkat kepatuhan ISO 27001/SNI. Pemberian rekomenasi perbikan hanya diberikan pada 19 skenario dari 50 risiko yang sudah diperoleh berdasarkan skenario yang sudah disetujui oleh pihak instnasi

Penelitian lain dilakukan oleh Firzah Abdullah Basyarahil pada tahun 2017 [26]. Penelitian ini dilakukan di Surabaya, Direktorat Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya, dengan menggunakan seluruh bagian indeks KAMI. Tujuan dari penelitian ini adalah untuk mengetahui tingkat kategori sistem elektronik yang

digunakan di DPTI ITS dan pentingnya kematangan keamanan informasi di DPTI ITS. Alasan dilakukannya penelitian ini dikarenakan ditemukannya beberapa celah dalam keamanan sistem informasi dan jaringan yang terbilang cukup berbahaya sehinga perlu dilakukannya evaluasi dan peningkatan tingkat keamanan pada DPTSI ITS Peneliti memberikan rekomendasi kepada DPTSI ITS berdasarkan hasil penelitian yang diperoleh.

Penelitian ini terlebih dahulu dilakukan dengan mengidentifikasi data yang dibutuhkan untuk tujuan penelitian. Metode pengumpulan data yang digunakan kemudian dengan mewawancarai narasumber yang mengetahui kondisi DPTSI ITS. Langkah selanjutnya adalah mengamati dengan mengamati langsung situasi di DPTSI ITS. Hasil yang diperoleh adalah gambar-gambar yang menunjukkan penerapan sistem manajemen keamanan informasi di DPTSI ITS. Metode selanjutnya adalah dengan melihat informasi yang diperoleh yaitu dokumen-dokumen yang digunakan untuk mendukung hasil wawancara. Berdasarkan hasil kajian yang telah dilakukan, penerapan keamanan informasi pada DPTSI ITS masih sangat kurang dan tergolong tidak layak menurut Indeks KAMI versi 3.1. Salah satu masukan yang diberikan adalah pemberian informasi untuk mengikuti petunjuk teknis dari petunjuk teknis yang dibuat oleh Kominfo mengenai penilaian Indeks KAMI.

Hasil dari penelitian ini menunjukan tingkat penggunaan sistem elektronik sebesar 26 dari total 50 yang menunjukan jika DPTSI ITS Surabaya memiliki ketergantungan yang tergolong tinggi dalam kebutuhan penggunaan sistem elektronik. Hasil dari penilaian Indeks KAMI pada DPTSI ITS sebesar 249 dari total jumlah keseluruhan sebesar 645 dengan berada pada level I-II yang menunjukan masih berada pada kondisi awal dalam penerapan keamanan informasi dan penerapan kerangka kerja dasar dalam penerapan keamanan informasi. Aspek yang mendapat nilai tertinggi adalah aspek Teknologi & Keamanan Informasi dengan poin sebesar 75. Sedangkan aspek yang mendapat nilai terendah adalah aspek Pengelolaan Risiko Keamanan Informasi dengan poin sebesar 24.

Penelitian lainnya dilakukan pada tahun 2019 oleh Shella Indah Dwi Octaviani, Suprapto, dan Admaja Dwi Herlambang [27]. Penelitian ini berisikan tentang evaluasi kesiapan kerangka kerja keamanan informasi menggunakan Indeks KAMI. Penelitian ini dilakukan pada Diskominfo Kota Batu dengan tujuan untuk mengetahui sejauh mana tingkat kesiapan keamanan informasi di Diskominfo Kota Batu. Penelitian ini harus dilakukan karena perlunya dilakukan evaluasi terhadap instansi pemerintahan setiap tahunnya. Hasil yang didapatkan adalah tingkat kesiapan kerangka kerja keamanan informasi di Diskominfo Kota Batu berada pada kategori rendah dan perlu dilakukan perbaikan. Dari hasil penelitian tersebut akan diberikan rekomendasi sesuai dengan hasil penelitian berdasarkan kontrol ISO 27001.

Penelitian diawali dengan melakukan wawancara pada bidang Teknologi Informasi dan Komunikasi terutama Seksi Keamanan Informasi dan Telekomunikasi. Lalu melakukan studi literatur yang bersumber dari buku, jurnal penelitian, dan paper. Metode selanjutnya adalah pengumpulan data dengan metode memilih responden yang tepat, lalu melakukan pengisian kuesioner yang dilakukan oleh responden yang sudah ditentukan, langkah selanjutnya adalah melakukan validasi data dengan metode *checklist* dengan tujuan memverifikasi data sesuai dengan keadaan sebenarnya. Metode berikutnya adalah mengkonfirmasi data dan menganalisis data yang sudah didapatkan dengan perhitungan Indeks KAMI dan melakukan perbandingan dengan ISO/IEC 27001:2013. Lalu metode selanjutnya adalah membuat rekomendasi perbaikan dan kesimpulan. Dari hasil kesimpulan tersebut maka akan didapatkan rekomendasi yang akan diberikan kepada pihak Diskominfo Kota Batu.

Hasil yang didapatkan dari penelitian ini menunjukan jika Diskominfo Kota Batu berada dalam kategoti rendah dengan jumlah skor sebesar 203 untuk tingkat kelengkapan dikarenakan belum diterapkan atau masih dalam tahap perencanan untuk semua syarat keamanan informasi dengan rata-rata area keamanan informasi berada oada level I sampai level I+. Dari hasil penilaian tersebut, dapat disimpulkan jika masih ada beberapa kontrol dalam ISO/IEC 27001:2013 yang belum memenuhi berdasarkan penilaian yang menggunakan Indeks KAMI.

Penelitian lainnya dilakukan oleh Fathoni Mahardika pada tahun 2017 [21]. Penelitian ini membahas tentang penilaian manajemen risiko keamanan informasi pada STMIK Sumedang dengan menggunakan metode *Framework* NIST SP 800-30 *Revision* 1. Tujuan dari dilakukan nya penelitian tersebut adalah untuk mengetahui nilai dari manajemen risiko keamanan informasi pada STMIK Sumedang dikarenakan STMIK Sumedang belum melakukan penilaian dan manajemen risiko keamanan informasi. Penelitian ini menunjukan bahwa STMIK Sumedang belum melakukan penilaian dan manajemen risiko keamanan informasi. Masih terdapat beberapa pengendalian agar risiko perusahaan dapat diminimalisir. Untuk level risiko keamanan informasi, STMIK Sumedang memiliki level risiko tingkat *Moderate* berdasarkan pada analisis kualitatif dan wawancara risiko keamanan informasi. Sedangkan untuk penilaian kematangan (*Maturity*) keamanan informasi berada pada nilai di kisaran 2,18 dengan kondisi tingkat keamanan yang ada hanya berupa perencanaan tanpa ada dokumentasi dan kontrol penanganan risiko berupa prosedur standar kebijakan keamanan.

Metode pertama yang digunakan adalah metode kualitatif yang digunakan untuk meneliti kondisi pada objek yang alamiah dengan studi kasus pada STMIK Sumedang. Metode selanjutnya adalah pengumpulan data yang dilakukan dengan 2 (dua) proses pengumpulan data, yaitu dengan metodologi pustaka dan metodologi lapangan. Metodologi Pustaka dilakukan dari beberapa referensi yang berupa buku, modul penelitian, modul perkuliahan, menelusuri *website* atau mencari sumber lainnya dari perpustakaan. Untuk metodologi lapangan, proses pengumpulan data yang digunakan adalah dengan wawancara atau *interview* dan observasi. Proses pengumpulan data dengan wawancara atau *interview* dilakukan secara langsung kepada pihak yang berkepentingan dalam perusahaan. Metode selanjutnya adalah dengan teknik analisis yang dilakukan dengan menggunakan spreadsheet pada Microsoft Excel dengan tujuan mengolah data aset TI yang berupa *software, hardware,* dan infrastruktur jaringan yang akan menghasilkan rekomendasi draft kebijakan keamanan informasi. Untuk alat penilitian yang digunakan dalam melakukan penelitian ini adalah NIST SP 800-30 *Revision* 1 dan ISO 27002:2005.

Penelitian yang dilakukan pada STMIK Sumedang menunjukan jika STMIK Sumedang memiliki level risiko keamanan informasi yang tergolong *Moderate*, yang terdiri dari risiko adversial terdiri dari: 20 *High*, 46 *Moderate*, 2 *Very Low*. Dan untuk risiko *non-adversarial* yang terdiri dari: 2 *Very high*, 5 *High*, 9 *Moderate*, 1 *Low*. Hasil penilaian ini didapatkan dari hasil analisis kualitatif dan wawancara risiko keamanan informasi. Untuk penilaian kematangan keamanan informasi mendapatkan nilai di kisaran 2,18 dikarenakan tingkatan keamanan janya direncanakan tanpa adanya dokumentasi dan kontrol penanganan risiko yang berbentuk sebuah prosedur kebijakan keamanan.

Penelitian lainnya dilakukan oleh Nurhafifah Matondang, Ika Nurlaili Isnaiiyah, dan Anita Muliwati pada tahun 2018 [28]. Penelitian ini bertujuan untuk menganalisis manajemen risiko keamanan data sistem informasi pada RSUD XYZ agar dapat mengukur besarnya ancaman dan kerentanan setiap data informasi, sehingga dapat meminimalisir dan mengatasi risiko pada bidang teknologi informasi.

Metode penelitian yang digunakan adalah metode OCTAVE Allegro dengan 8 langkah utama. Langkah pertama yang dilakukan adalah membangun kriteria pengukuran risiko. Langkah ini terdiri dari dua aktivitas, yaitu dengan membuat definisi dari ukuran kuantitatif dan didokumentasikan pada *Risk Measurement Criteria Worksheet*. Lalu aktivitas kedua adalah dengan memberikan nilai prioritas pada *impact area* dengan menggunakan *Impact Area Ranking Worksheet*. Langkah kedua adalah dengan mengembangkan profil pada aset informasi yang terdiri dari 8 aktivitas. Aktivitas pertama diawali dengan mengidentifikasi aset informasi. lalu dilanjutkan dengan penilaian risiko terstruktur pada aset yang terbilang kritis, lalu dilakukan pengumpulan informasi mengenai *information asset* yang penting, lalu dilanjutkan dengan pembuatan dokumentasi alasan pemilihan aset informasi kritis. Aktivitas selanjutnya adalah membuat penjelasan tentang aset informasi yang kritis tersebut, lalu mengisi kebutuhan keamanan sesuai dengan aspek *confidentially*, *integrity*, dan *availability*. Lalu aktivitas terakir adalah mengidentifikasi kebutuhan keamanan terpenting pada aset informasi. Langkah ketiga adalah mengidentifikasi

container dari aset informasi yang berdasar pada tiga poin penting yaitu tingkat perlindungan, pengamanan aset informasi, dan kerentanan serta ancaman pada *container* aset informasi. Langkah keempat adalah mengidentifikasi area masalah, langkah ini terdiri dari empat aktivitas yang diawali dengan pengembangan profil risiko pada aset informasi yang dilakukan dengan cara bertukar pikiran dengan tujuan mencari faktor ancaman yang berasal dari situasi yang mungkin akan mengancam aset dan dilakukan dengan pedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* yang akan tercatat pada *area of concern* yang selanjutnya akan dilakukan reviu dari *container* dengan tujuan membuat dan mendokumentasikan *Area of Concern*. Langkah kelima adalah mengidentifikasi skenario ancaman yang dilakukan dengan melakukan identifikasi skenario ancaman tambahan dengan menggunakan *Threat Scenario Questionaries*, lalu melengkapi *Information Asset Risk Worksheet* pada setiap skenario ancaman umum. Langkah keenam adalah mengidentifikasi risiko dengan cara menentukan *threat scenario* berdasarkan pada *Information Asset Risk Worksheet* yang telah didokumentasikan yang dapat memberikan dampak bagi organisasi. Langkah ketujuh adalah melakukan analisa risiko yang dilakukan dengan mengacu pada dokumentasi pada *Information Asset Risk Worksheet*, langkah ini dimulai dengan melakukan reviu pada *risk measurement criteria* dan dilanjutkan dengan penghitungan pada nilai risiko relatif yang akan digunakan untuk melakukan analisis risiko. Lalu langkah kedelapan adalah memilih pendekatan pengurangan, langkah ini dimulai dengan mengurutkan setiap risiko yang telah diidentifikasi berdasar pada nilai risikonya yang bertujuan untuk membantu pengambilan keputusan status untuk mitigasi risiko tersebut, lalu aktivitas selanjutnya adalah dilakukannya pendekatan mitigasi dari setiap risiko dengan pedoman pada kondisi unik dalam organisasi tersebut dan dilakukan dengan koordinasi lebih lanjut dengan pihak manajemen dari Rumah Sakit Umum Daerah XYZ.

Hasil dilakukannya penelitian ini adalah RSUD XYZ sudah menerapkan metode OCTAVE Allegro untuk penilaian pada aset informasi yang bersifat kritis beserta dengan ancaman dan risiko yang mungkin terjadi. Hasil dari dilakukannya

evaluasi pada lima impact areas menunjukan reputasi dan kepecayaan pelanggan memiliki nilai tertinggi dengan nilai 12 (*medium*) dengan perbandingan *relative risk score* dengan nilai 27. Keseluruhan hasil dapat menunjukan jika data-data tentang pasien merupakan aset informasi bersifat kritis sehinga diperlukannya upaya perencanaan untuk dilakukan penanganan dan mitigasi risiko.

Penjelasan mengenai penelitian yang sudah dijelaskan di atas akan diringkas pada tabel 2.1 berikut ini.

Tabel 2. 6 Perbandingan dengan Penelitian Sebelumnya

No	Peneliti	Tahun	Tujuan	Alat	Hasil
1	I Putu Setyo Syahindra, Clara Hetty Primasari, Aloysius Bagas Pradipta Irianto	2015	Mengetahui tingkat risiko keamanan informasi di Dinas Komunikasi dan Informasi Provinsi XYZ dan memberikan rekomendasi kepada Dinas Komunikasi dan Informasi Provinsi XYZ	Indeks KAMI & ISO 27005:2011	Dinas Komunikasi dan Informasi Provinsi XYZ memiliki nilai kelengkapan sebesar 457 yang termasuk "Cukup Baik" untuk memenuhi standar ISO/IEC 27001.
2	Firzah Abdullah Basyarahil	2017	Mengetahui tingkat kategori sistem	Indeks KAMI	Penerapan keamanan informasi di DPTSI ITS masih terbilang sangat

			elektronik pada DPTSI ITS dan mengetahui nilai maturitas keamanan informasi di DPTSI ITS.		kurang dan tergolong tidak layak sesuai dengan Indeks KAMI versi 3.1. Salah satu masukkan yang diberikan adalah memberi masukkan untuk mengikuti petunjuk teknis dari Bimbingan Teknis yang sudah dilaksanakan oleh pihak Kominfo mengenai penilaian pada Indeks KAMI.
3	Shella Indah Dwi Octaviani, Suprapto, Admaja Dwi Herlambang	2019	Mengetahui sejauh mana nilai evaluasi kesiapan kerangka kerja keamanan informasi di Diskominfo Kota Batu	Indeks KAMI	Nilai evalasi kesiapan kerangka kerja keamanan informasi di Diskominfo Kota Batu berada pada kategori rendah dan perlu dilakukan perbaikan. Dari penelitian tersebut akan diberikan rekomendasi sesuai dengan hasil penelitian

					berdasarkan kontrol ISO 27001.
4	Fathoni Mahardika	2017	Mengetahui nilai dari manajemen risiko keamanan informasi pada STMIK Sumedang	NIST SP 800-30 *Revision* 1	STMIK Sumedang belum melakukan penilaian dan manajemen risiko keamanan informasi. Masih terdapat beberapa pengendalian agar risiko perusahaan dapat diminimalisir. Untuk level risiko keamanan informasi, STMIK Sumedang memiliki level risiko tingkat *Moderate*. Penilaian kematangan (*Maturity*) keamanan informasi berada pada nilai di kisaran 2,18 dengan kondisi tingkat keamanan yang ada hanya berupa perencanaan tanpa ada dokumentasi dan kontrol

					penanganan risiko berupa prosedur standar kebijakan keamanan.
5	Nurhafifah Matondang, Ika Nurlaili Isnainiyah, Anita Muliawati	2018	Menganalisis manajemen risiko keamanan data sistem informasi pada RSUD XYZ	OCTAVE Allegro	Hasil dari dilakukannya evaluasi pada lima *impact areas* menunjukan reputasi dan kepecayaan pelanggan memiliki nilai tertinggi dengan nilai 12 (*medium*) dengan perbandingan *relative risk score* dengan nilai 27. Keseluruhan hasil dapat menunjukan jika data-data terkait tentang pasien merupakan aset informasi bersifat kritis sehinga diperlukannya upaya perencanaan untuk dilakukan penanganan dan mitigasi risiko.

6	Felix Maximillian Tanardi	2021	Mengevaluasi pengelolaan risiko keamanan informasi di Diskominfo XYZ	Indeks KAMI	