BAB II

LANDASAN TEORI

2.1 Keamanan Informasi dan Sistem Manajemen Keamanan Informasi

2.1.1 Keamanan Informasi

Informasi merupakan *asset* berharga yang dimiliki oleh perusahaan untuk dapat mengambil keputusan dalam keberlanjutan bisnis, oleh karena itu suatu perusahaan perlu melindungi informasi agar tidak di salah gunakan oleh orang yang tidak berwenang. Adapun cara untuk dapat melindungi informasi dengan cara menerapkan keamanan informasi [19]. Keamanan informasi sendiri merupakan perlindungan segala jenis sumber daya informasi terhadap pihak-pihak yang tidak berwenang dalam mengelola informasi tersebut, dimana upaya perlindungan keamanan informasi memiliki tujuan yaitu untuk memastikan dan menjamin keberlangsungan bisnis (*business continuity*), mengurangi risiko bisnis (*reduce business risk*), dan mengoptimalkan keuntungan atau pengembalian investasi dan peluang bisnis (*return of investment*) [20].

Gambar 2. 1 Aspek Keamanan Informasi
Sumber: [20]

Pada Gambar 2.1 merupakan 3 aspek dalam keamanan informasi yang perlu diperhatikan oleh suatu perusahaan atau organisasi, dimana aspek tersebut yaitu:

a. ***Confidentiality***

Kerahasiaan memiliki pengertian yaitu sebagai suatu properti bahwa data atau informasi tidak diungkapkan kepada individu, entitas, atau proses yang tidak sah. Selain itu, kerahasiaan juga perlu dijaga dari pihak-pihak tidak berwenang agar informasi atau data tidak bocor. Sehingga, *confidentiality* atau kerahasiaan merupakan aspek yang memastikan atau menjamin kerahasiaan data atau informasi hanya dapat diakses oleh orang yang memiliki wewenang atas data atau informasi tersebut. Selain itu, aspek ini juga menjamin kerahasiaan data atau informasi yang terkirim, diterima, dan disimpan.

b. ***Integrity***

Integritas memiliki hubungan dengan akurasi atau kelengkapan data serta informasi, dimana data atau informasi yang terdapat dalam suatu perusahaan atau organisasi perlu dijaga keakuratan, kebenaran, dan kelengkapannya. Sehingga, *integrity* atau integritas merupakan aspek yang menjamin bahwa data atau informasi tidak dapat diubah apabila tidak terdapat izin dari pihak yang berwenang. Selain itu, aspek ini menjamin bahwa data atau informasi dijaga keutuhannya, serta dijaga dari kerusakan atau ancaman yang dapat menyebabkan perubahan nilai dari data atau informasi yang asli.

c. ***Availability***

Ketersediaan merupakan kemudahaan untuk seorang *user* yang berwenang dalam mengakses data atau informasi tanpa adanya gangguan. Sehingga, *availability* atau ketersediaan merupakan aspek yang menjamin bahwa data atau informasi akan selalu tersedia, serta dapat diakses dimanapun dan kapanpun *user* yang berwenang membutuhkan tanpa adanya gangguan [21].

2.1.2 Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) merupakan sistem manajemen yang memiliki kaitan dengan penerapan keamanan informasi di dalam suatu perusahaan atau organisasi. Dimana sistem manajemen tersebut meliputi kegiatan perancangan, penerapan, dan pemeliharaan terhadap keamanan informasi dalam suatu perusahaan. Suatu perusahaan perlu untuk menerapkan Sistem Manajemen Keamanan Informasi, hal tersebut dikarenakan agar informasi yang terdapat dalam perusahaan atau organisasi dapat dikelola dengan baik agar dapat menghasilkan data untuk perusahaan dalam mengambil keputusan. Adapun tujuan dari Sistem Manajemen Keamanan Informasi (SMKI) yaitu untuk meminimalisir risiko serta menjamin keberlangsungan bisnis secara proaktif, hal ini bermaksud agar dapat membatasi dampak yang terjadi karena pelanggaran keamanan [22].

2.2 *Framework* ISO 27001

2.2.1 The International Organization for Standardization (ISO)

ISO atau *The International Organization for Standardization* adalah badan organisasi internasional yang memiliki anggota dari 167 badan standar nasional di dunia, dimana dari seluruh anggota yang ada dikumpulkan untuk membagikan pengetahuan. Dari pengetahuan yang dikumpulkan maka dikembangkan menjadi sebuah ketentuan atau standar yang berlaku secara internasional yang sesuai dengan pasar kelas dunia. Tujuan dibentuknya ISO adalah agar perusahaan atau organisasi mengetahui standar internasional untuk dapat bersaing dengan pasar global [17]. Adapun beberapa manfaat apabila suatu perusahaan atau organisasi memiliki standar ISO, seperti meningkatkan citra perusahaan, mengurangi risiko usaha, meningkatkan kinerja lingkungan perusahaan, mendapat kepercayaan dari konsumen atau mitra kerja, meningkatkan daya saing, dan lainnya.

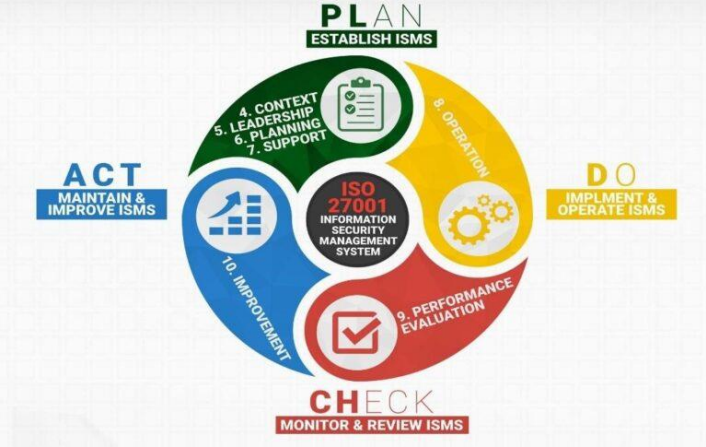
Standar ISO yang dikeluarkan memiliki banyak macam jenis yang disesuaikan pada bidang tertentu, berikut merupakan beberapa jenis ISO yang terkenal yaitu ISO 9001 yang merupakan standar internasional yang menetapkan standar untuk sistem manajemen mutu, ISO 31000 yang merupakan standar internasional yang menetapkan standar untuk manajemen risiko, ISO 45000 yang merupakan standar internasional yang menetapkan standar untuk sistem manajemen kesehatan dan keselamatan kerja (SMK3), ISO 27001 yang merupakan standar internasional yang menetapkan standar untuk Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS).

2.2.2 ISO 27001 Versi 2013

ISO 27001 merupakan standar yang dibentuk oleh badan organisasi internasional ISO, standar ini sudah diakui dan diadopsi oleh seluruh dunia termasuk Indonesia [23]. Standar ini tidak bergantung pada produk teknologi informasi tertentu, membutuhkan pendekatan manajemen yang didasarkan pada risiko, serta dirancang untuk memastikan bahwa kontrol keamanan yang dipilih nantinya dapat melindungi aset informasi dari berbagai risiko dan memberikan keyakinan mengenai tingkat keamanan kepada pihak yang terkait [24]. ISO 27001 sendiri berisi mengenai spesifikasi atau persyaratan dasar yang perlu dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI) dalam suatu organisasi.

2.2.3 *Plan-Do-Check-Act* (PDCA)

ISO 27001 dikembangkan dengan mengadopsi model PDCA atau *Plan-Do-Check-Act*, yang dimana model tersebut digunakan oleh Sistem Manajemen Keamanan Informasi (SMKI) sebagai metode evaluasi. Adapun pada Gambar 2.2 merupakan model PDCA yang diadopsi dalam ISO 27001.



Gambar 2. 2 Siklus Plan-Do-Check-Act
Sumber: [25]

Metode *Plan-Do-Check-Act* merupakan metode yang diperkenalkan oleh Dr. W. Edwards Deming, dimana metode tersebut juga biasa disebut dengan siklus deming. Terdapat 4 tahapan pada metode ini, sebagai berikut:

a. ***Plan***

Tahapan *plan* merupakan tahapan merencanakan, dimana pada tahapan ini meliputi pembentukan tim dan pelatihan, ditetapkan suatu target atau sasaran yang ingin dicapai dalam suatu proses atau permasalahan yang ingin dipecahkan, serta batasan waktu yang diperlukan dalam menjalani perencana yang ada. Tujuan adanya tahapan ini adalah agar mempermudah suatu pengerjaan masalah agar lebih terarah. Pada evaluasi Sistem Manajemen Keamanan Informasi, tahapan ini membantu untuk menetapkan ruang lingkup objektif hingga mengidentifikasi masalah yang terjadi dalam suatu perusahaan terkait Sistem Manajemen Keamanan Informasi baik internal maupun eksternal.

b. ***Do***

Tahapan *do* merupakan tahapan melaksanakan, dimana pada tahapan ini menjalankan atau menerapkan semua perencanaan yang telah direncanakan di tahapan sebelumnya (*plan*). Selain menjalankan perencanaan, pada tahapan ini juga dilakukan

pengumpulan data yang nantinya data tersebut berguna untuk tahapan selanjutnya. Pada evaluasi Sistem Manajemen Keamanan Informasi, tahapan ini membantu untuk melakukan evaluasi di suatu perusahaan, pada tahapan ini dipastikan evaluasi yang dilakukan sesuai dengan kebijakan yang ada.

c. ***Check***

Tahapan *check* merupakan tahapan pemeriksaan, dimana pada tahapan diharapkan dilakukan pemeriksaan dan peninjauan ulang terhadap hasil-hasil yang didapatkan dari tahapan sebelumnya (*do*). Selain itu, pada tahapan ini dilakukan perbandingan terhadap hasil aktual yang telah dicapai dengan target yang diharapkan pada tahapan *plan*. Tujuan dilakukannya tahapan ini adalah untuk memeriksa kembali masalah yang diidentifikasi sebelumnya. Pada evaluasi Sistem Manajemen Keamanan Informasi, tahapan ini membantu untuk memantau, mengukur, menganalisis, serta memeriksa evaluasi yang telah dilakukan.

d. ***Act***

Tahapan *act* merupakan tahapan tindakan lanjut, dimana pada tahapan ini menindaklanjuti hasil yang telah didapatkan dari tahapan sebelumnya (*check*). Dari hasil pemeriksaan maka didapatkan aspek atau masalah yang perlu diperbaiki agar dapat memenuhi target yang telah ditetapkan. Selain itu, apabila dari hasil yang telah didapatkan sudah sesuai dengan target, maka adapun tindakan yang dilakukan yaitu tindakan standarisasi. Tindakan standarisasi ini merupakan tindakan untuk menstandarkan solusi yang dapat dilakukan apabila terdapat masalah serupa. Pada evaluasi Sistem Manajemen Keamanan Informasi, tahapan ini digunakan untuk melakukan tindakan perbaikan serta pencegahan yang sesuai dengan kebijakan Sistem Manajemen Keamanan Informasi yang digunakan.

Ketika keempat tahapan sudah selesai, maka akan dilakukan pengulangan siklus yang dimulai dari tahapan *plan*, dimana tujuan dilakukannya siklus yang berulang ini dapat berguna untuk mengembangkan perusahaan agar menjadi lebih baik lagi [25].

2.3 *Tools* Indeks Keamanan Informasi (KAMI)

2.3.1 Indeks KAMI

Dalam membantu proses evaluasi ISO 27001:2013, digunakan alat bantu atau *tools* Indeks KAMI, dimana Indeks KAMI adalah alat bantu dalam melakukan evaluasi untuk menganalisis tingkat kematangan dan kesiapan keamanan informasi suatu perusahaan. Indeks KAMI sendiri telah rancang dan disesuaikan dengan standar internasional yaitu ISO 27001 versi 2013. Indeks KAMI juga telah di *design* agar dapat digunakan oleh seluruh perusahaan atau instansi dari segala ragam tingkatan, ukuran, atau tingkat kepentingan penggunaan TIK untuk mendukung terlaksananya proses yang ada pada perusahaan [18]. Dengan suatu perusahaan menggunakan Indeks KAMI sebagai *tools* evaluasi maka nantinya perusahaan akan mendapatkan gambaran kondisi kesiapan *framework* keamanan informasi pada perusahaan, dimana alat ini juga dapat digunakan secara berkala. Adanya gambaran tersebut dapat membantu suatu perusahaan dalam meningkatkan keamanan informasi dalam perusahaannya agar sesuai dengan standar atau kebijakan yang telah ditentukan [26].

2.3.2 Evaluasi Indeks KAMI

Dalam melakukan evaluasi menggunakan Indeks KAMI, maka adapun pertanyaan yang diberikan sesuai dengan kebutuhan penilaian pada tiap area, area tersebut yaitu:

a. Kategori Sistem Elektronik yang digunakan perusahaan
b. Tata Kelola Keamanan Informasi
c. Pengelolaan Risiko Keamanan Informasi

d. Kerangka Kerja Keamanan Informasi
e. Pengelolaan Aset Informasi
f. Teknologi dan Keamanan Informasi
g. Suplemen (tambahan pengukuran dilakukan untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan (Cloud Service) dan Perlindungan Data Pribadi.) [18].

Adapun pertanyaan dalam Indeks KAMI dibagi kedalam 2 kelompok keperluan, yaitu:

a. Berdasarkan kategori tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang ada pada ISO 27001:2013 serta kesiapan minimum sebagai prasyarat melakukan sertifikasi ISO 27001:2013. Kategori ini dibagi menjadi 3 label yaitu pada label “1” mengenai area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi, label “2” mengenai efektifitas dan konsistensi penerapannya, serta lebal “3” mengenai kemampuan dalam meningkatkan kinerja keamanan informasi. Setiap pertanyaan diberikan penilaian yang nantinya dapat menghasilkan angka Indeks, berikut merupakan pemetaan skor Indeks KAMI:

	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

Gambar 2. 3 Pemetaan Skor Area Pengamanan
Sumber: Indeks KAMI [26]

Pada Gambar 2.3 merupakan pemetaan skor untuk keseluruhan area pengamanan, dengan catatan yaitu untuk pengisian untuk mendapatkan hasil dari label "3", semua pertanyaan yang terkait dengan label "1" dan "2" harus dijawab dengan status minimal "Diterapkan Sebagian" [26].

b. Berdasarkan kategori tingkat kematangan penerapan keamanan dengan kategori yang merujuk pada tingkat kematangan yang digunakan oleh *framework* atau kerangka kerja yang nantinya digunakan sebagai alat untuk menggambarkan pemeringkatan kesiapan keamanan informasi dalam suatu perusahaan [18]. Untuk mengetahui tingkat kematangan ada kategori ini, dilakukan penilaian terhadap 5 area yang sesuai dengan kondisi kematangan informasi sesuai standar ISO 27001:2013. Kelima area tersebut yakni:

- Tata Kelola Keamanan Informasi,
- Pengelolaan Risiko Keamanan Informasi,
- Kerangka Kerja Keamanan Informasi,
- Pengelolaan Aset Informasi, dan
- Teknologi dan Keamanan Informasi.

2.3.3 Penilaian Indeks KAMI

2.3.3.1 Kategori I: Sistem Elektronik

Untuk mengetahui kesiapan pengamanan informasi pada suatu perusahaan, adapun Kategori I yang dapat membantu mengetahui kesiapan tersebut. Kategori ini merupakan kategori yang melakukan penilaian terhadap Sistem Elektronik. Dilakukan penilaian ini berguna untuk mengetahui bagaimana tingkat Sistem Elektronik pada suatu instansi atau perusahaan. Maksud dari mengetahui definisi Sistem Elektronik ini berguna untuk perusahaan dalam mengategorikan Sistem Elektronik yang digunakan berdasarkan tingkatnya. Terdapat 3 tingkatan pada penilaian ini yaitu “Rendah”, “Tinggi”, dan “Strategis”. Untuk dapat mengetahui tingkatan atau *leve* tersebut maka diperlukan pengisian terhadap penilaian dari beberapa pertanyaan, dimana pertanyaan diisi dengan status yang tersedia yaitu “A”, “B”, atau “C”, dimana status tersebut memiliki skor-nya masing masing. Penilaian untuk status “A” memiliki skor 5,

status “B” memiliki skor 2, dan untuk status “C” memiliki skor yaitu 1 [26].

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**	Skor
#	**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	A	5
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	A	5
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	A	5
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi	B	2

Gambar 2. 4 Tampilan Indeks KAMI Kategori Sistem Elektronik
Sumber: Indeks KAMI [26]

Gambar 2.4 merupakan tampilan Indeks KAMI untuk kategori tingkat kesiapan terhadap sistem elektronik. Pertanyaan pada kategori ini meliputi:

a. Nilai investasi untuk Sistem Elektronik (SE) yang terdapat pada perusahaan,
b. Total anggaran yang dialokasikan perusahaan untuk pengelolaan SE,
c. Kewajiban terhadap standar atau peraturan yang ada pada perusahaan,
d. Penggunaan teknik kriptografi khusus dalam Sistem Elektronik untuk Keamanan Informasi perusahaan,
e. Jumlah penggunaan SE pada perusahaan,
f. Data pribadi yang dikelola SE pada perusahaan,
g. Tingkat klasifikasi data SE yang terdapat pada perusahaan,
h. Tingkat kritis porses yang ada dalam SE perusahaan,
i. Dampak dari kegagalan SE pada perusahaan, dan
j. Potensi kerugian apabila terjadi insiden ditembusnya Keamanan Informasi SE pada perusahaan [26].

Setelah mengisi pertanyaan tersebut nantinya dapat dilakukan pemetaan skor untuk mengetahui tingkat peran Sistem Elektronik pada perusahaan.

Rendah	
10	15
Tinggi	
16	34
Strategis	
35	50

Gambar 2. 5 Pemetaan Tingkatan Berdasarkan Skor
Sumber: Indeks KAMI [26]

Pada Gambar 2.5 merupakan pemetaan tingkat Sistem Elektronik pada perusahaan berdasarkan perolehan nilai skor, dimana hasil penilaian dijabarkan ke dalam tiga kategori tingkatan yaitu Rendah, Tinggi, dan Strategis. Dimana tingkat Rendah didapatkan apabila perusahaan mendapatkan penilaian dengan perolehan skor 10-15, dimana maksudnya adalah penggunaan Sistem Elektronik pada perusahaan mendukung proses kerja yang berjalan meskipun tidak pada tingkatan yang signifikan. Selanjutnya tingkat Tinggi didapatkan apabila perusahaan mendapatkan penilaian dengan perolehan skor 16-34, maksudnya adalah penggunaan SE pada perusahaan merupakan hal yang tidak dipisahkan. Sistem Elektronik dengan proses kerja yang berjalan sejalan dan tidak dapat dipisahkan. Terakhir yaitu tingkat Strategis, tingkatan ini didapatkan apabila perusahaan mendapatkan penilaian dengan perolehan skor 35-60, dimana memiliki pengertian yaitu proses kerja hanya dapat dilakukan melalui penggunaan Sistem Elektronik di dalam perusahaan [26].

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. 6 Korelasi Kesiapan dengan kategori Sistem Elektronik
Sumber: Indeks KAMI [26]

Gambar 2.6 merupakan korelasi antara status kesiapan dengan kategori Sistem Elektronik.

2.3.3.2 Kategori Tingkat Kematangan

Tingkat kematangan merupakan penilaian terhadap enam area, pada kategori ini tingkat kematangan didefinisikan menjadi 5 tingkatan yaitu:

Tabel 2. 1 Definisi Tingkat Kematangan (TK)

Tingkat I	Kondisi Awal
Tingkat II	Penerapan Kerangka Kerja Dasar
Tingkat III	Terdefinisi dan Konsisten
Tingkat IV	Terkelola dan Terukur
Tingkat V	Optimal

Pada Tabel 2.1 merupakan uraian mengenai definisi tingkat kematangan. Namun, untuk lebih detail lagi uraian mengenai tingkatan kematangan ditambah lagi dengan menjadi I+, II+, III+, dan IV+. Maka dari itu, tingkat kematangan yang terdefinisi totalnya adalah 9 tingkat. Awalnya Indeks KAMI akan secara otomatis terdapat pada kategori kematangan Tingkat I. Namun, untuk dapat mengikuti sertifikasi ISO 27001 terdapat tingkat kematangan minimum yang perlu dipenuhi yaitu pada tingkat III+. Untuk mendapatkan tingkatan tersebut, maka diperlukan pengisian atas pertanyaan dari kelima area yang ada.

Gambar 2. 7 Tampilan Salah Satu Area Kategori Tingkat Kematangan
Sumber: Indeks KAMI

Gambar 2.7 merupakan tampilan pada salah satu area atau kategori dalam penilaian tingkat kematangan, dimana dalam gambar tersebut terdapat beberapa kolom. Berikut merupakan pengertian di tiap kolom:

(1) Kolom 1 (Hitam) : Kategori kematangan

Pada kolom ini merupakan kategori kematangan, dimana tingkat kematangan sendiri terdapat 3 tingkat yaitu Tingkat Kematangan II, III, dan IV. Dimana disetiap tingkatan memiliki minimal skornya dan skor pencapaian kematangannya masing-masing serta berbeda di setiap areanya. Untuk tahap III dan IV terdapat penilaian validitas apabila skor penilaian tingkat kematangan di tingkat II memenuhi skor pencapaian tingkat kematangan tingkat II. Setelah mengisi seluruh pertanyaan nantinya akan muncul skor kematangan dan statusnya.

(2) Kolom 2 (Merah) : Kategori tahap penerapan

Pada kolom ini merupakan kategori tahap penerapan, dimana terdapat 3 tahap yaitu tahap 1, 2, dan 3. Tahap ini memiliki minimal skor yang di tiap area memiliki minimal skor yang berbeda. Dimana skor tahap 3 akan terlihat apabila skor tahap penerapan 1 dan 2 diisi dan memenuhi minimal skor.

(3) Kolom 3 (Kuning) : Daftar pertanyaan

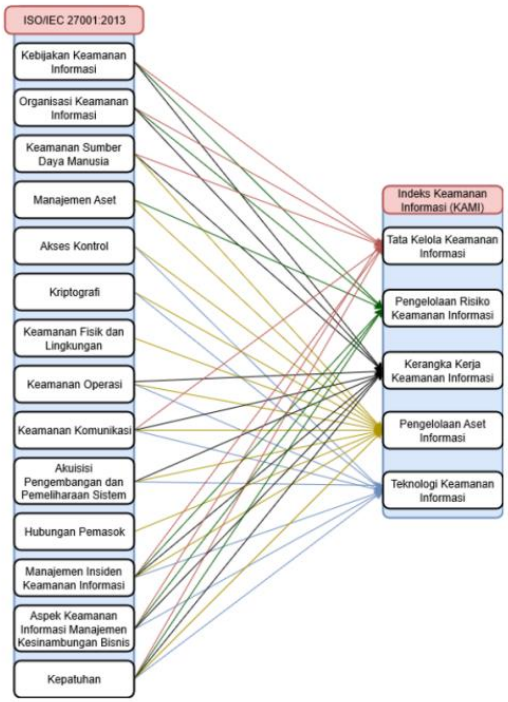
Pada kolom ini disediakan pertanyaan-pertanyaan yang perlu dijawab agar dapat menghasilkan penilaian atau skor tingkat kematangan.

(4) Kolom 4 (Hijau) : Pilihan Status

Pada kolom ini tersedia pilihan jawaban atas pertanyaan yang diajukan, pilihan jawaban ini dibagi menjadi 4 status yaitu "Tidak Dilakukan", "Dalam Perencanaan", "Dalam Penerapan/Diterapkan Sebagian", dan "Diterapkan Secara Menyeluruh". Setiap status memiliki nilai masing-masing, tergantung pada tingkat kematangan dan tahapan yang terkait [26].

2.3.4 Hubungan Indeks KAMI dengan ISO 27001 versi 2013

Indeks KAMI merupakan *tools* yang di *design* berdasarkan standar ISO 27001 versi 2013, dimana area yang terdapat pada Indeks KAMI dibuat berdasarkan dengan standar ISO 27001:2013.



Gambar 2. 8 Hubungan Indeks KAMI Versi 3 dengan ISO 27001:2013
Sumber: Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer [27]

Pada Gambar 2.8 merupakan korelasi antara Indeks KAMI versi 3 dengan ISO 27001:2013. Indeks KAMI membuat rangkuman atas 14 area kontrol pada ISO 27001:2013 terkait Keamanan Informasi menjadi 5 area, namun terdapat penambahan kategori baru yaitu Kategori VII: Suplemen yang dimana kategori ini membahas mengenai aspek kesiapan pengamanan atau keterlibatan pihak ketiga. Sehingga, berikut merupakan hubungan antara Indeks KAMI versi 4 dengan ISO 27001:2013,

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi	Suplemen
Security Policies	√	√	√			√
Organisation of Information Security	√	√	√			
Human Resource Security	√		√	√		√
Asset Management		√		√		√
Access Control				√	√	√
Cryptography				√	√	√
Physical and Environmental Security				√		
Operations Security			√	√	√	√
Communications Security	√		√	√	√	√
Systems Acquisition, Development and Maintenance			√	√	√	
Supplier Relationships				√		
Information Security Incident Management	√	√	√	√	√	√
Information Security Aspects of BCM	√	√	√		√	√
Compliance	√	√	√	√	√	√

Gambar 2. 9 Hubungan Indeks KAMI Versi 4 dengan ISO 27001:2013
Sumber: Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer [28]

Pada Gambar 2.9 terlihat korelasi antara masing-masing area yang terdapat di Indeks KAMI berdasarkan ISO 27001 versi 2013. Adapun berikut adalah uraian pemetaan antara Indeks KAMI dengan ISO 2700 versi 2013:

Tabel 2. 2 Hubungan Indeks KAMI dengan ISO 27001:2013

No	Area Indeks Keamanan Informasi (KAMI)	Area Kontrol ISO 27001:2013
1	Kategori II: Tata Kelola Keamanan Informasi	- *Information Security Policy,* - *information Security Organization,* - *Human Resources,* - *Communication Security,* - *Information Security Incident Management,* - *Information Security Aspects of BCM, and* - *Compliance.*
2	Kategori III: Pengelolaan Risiko Keamanan Informasi	- *Information Security Policy,* - *information Security Organization,* - *Asset Management,* - *Information Security Incident Management,* - *Information Security Aspects of BCM, and* - *Compliance.*
3	Kategori IV: Kerangka Kerja Keamanan Informasi	- *Information Security Policy,* - *information Security Organization,* - *Human Resources,* - *Operations Security* - *Communication Security,* - *System Acquisition, Development and Maintenance,* - *Information Security Incident Management,* - *Information Security Aspects of BCM, and* - *Compliance.*
4	Kategori V: Pengelolaan Aset Informasi	- *Human Resources,* - *Asset Management,* - *Access Control,* - *cryptography,* - *Physical and Environmental Security,* - *Operations Security,* - *Communication Security,*

No	Area Indeks Keamanan Informasi (KAMI)	Area Kontrol ISO 27001:2013
		- *System Acquisition, Development and Maintenance,* - *Supplier Relations,* - *Information Security Incident Management,* - *Compliance.*
5	Kategori VI: Teknologi dan Keamanan Informasi	- *Access Control,* - *cryptography,* - *Operations Security,* - *Communication Security,* - *System Acquisition, Development and Maintenance,* - *Information Security Incident Management,* - *Information Security Aspects of BCM, and* - *Compliance.*
6	Kategori VII: Suplemen	- *Information Security Policy,* - *Human Resources,* - *Asset Management,* - *Access Control,* - *cryptography,* - *Operations Security,* - *Communication Security,* - *Information Security Incident Management,* - *Information Security Aspects of BCM, and* - *Compliance.*

2.4 Penelitian Terdahulu

Adapun dalam penulisan penelitian ini dilakukan penelitian terdahulu terhadap 5 jurnal, yang dilampirkan sebagai berikut:

Tabel 2. 3 Detail Jurnal Penelitian Terdahulu

No	Detail Jurnal	
1	Penulis	Piski Sundari dan Wella
	Jurnal	Ultima InfoSys: Jurnal Ilmu Sistem Informasi, Vol. 12, No. 1

No	Detail Jurnal	
	Tahun	2021
	Judul Artikel	SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR) [12]
	Permasalahan	Pusdatin merupakan lembaga pemerintah namun Pusdatin belum pernah melakukan penerapan standarisasi Keamanan Informasi dan evaluasi terhadap Tata Kelola Keamanan Informasi.
	Metode	Standar ISO 27001 versi 2013 *Tools* Indeks KAMI Siklus *Check-Act-Plan-Do* (CAPD)
	Hasil dan Kesimpulan	Pusdatin belum layak untuk melakukan sertifikasi ISO 27001:2013, dan masih memerlukan perbaikan, hal ini dikarenakan: a. Tingkat kepentingan TIK di Pusdatin adalah sebesar 39, dimana nilai tersebut termasuk dalam kategori "KRITIS". b. Hasil evaluasi pada 5 area Indeks KAMI menunjukkan bahwa Pustadin berada pada level atau tingkat kematangan I+, level tersebut berarti Pusdatin memerlukan "Perbaikan" keamanan informasi. Oleh karena itu, dapat disimpulkan bahwa Pusdatin masih rentan terhadap kejahatan yang mungkin dapat berisiko seperti terganggunya pelayanan sistem informasi di Pusdatin.
2	Penulis	Dicky Insan Khamil, Gusti Made Arya Sasmita, dan Anak Agung Ngurah Hary Susila
	Jurnal	Jurnal Teknik Informatika dan Sistem Informasi Vol. 9, No. 3, September 2022, Hal. 1948-1960
	Tahun	2022
	Judul Artikel	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar) [29]
	Permasalahan	Diperlukan evaluasi oleh Dinas Komunikasi dan Informatika Kabupaten Gianyar terkait Keamanan Informasi guna mencegah adanya risiko yang mengancam data atau informasi, serta memastikan Keamanan Informasi yang dikelola dan diterapkan oleh instansi sudah sesuai dengan prosedur dan memiliki performa yang maksimal.
	Metode	Standar ISO 27001 versi 2013 *Tools* Indeks KAMI Siklus *Plan-Do-Check-Act* (PDCA)

No	Detail Jurnal	
	Hasil dan Kesimpulan	Dinas Komunikasi dan Informatika Kabupaten Gianyar belum dinyatakan layak dalam memenuhi standar pada ISO 27001, hal ini karena: a. Dinas Komunikasi dan Informatika Kabupaten Gianyar mendapatkan skor akhir pada kategori sistem elektronik sebesar 34, dimana nilai tersebut dikategorikan "Tinggi", selain itu adapun skor akhir pada kategori keamanan informasi yaitu sebesar 190. b. Tingkat kematang berada pada tingkat II+. Oleh karena itu, dapat disimpulkan bahwa penerapan keamanan informasi pada institute tersebut berada pada area teknologi dan keamanan informasi, hal ini didapatkan karena hasil evaluasi pada area tersebut mendapatkan nilai paling mendekati kepatuhan standar dari ISO 27001, dan untuk area lainnya masih memerlukan perbaikan terutama pada area pengelolaan risiko dan area kerangka kerja
3	Penulis	Yuli Haryanto dan Reza Avrizal
	Jurnal	Jurnal Format Volume 8 Nomor 1 Tahun 2019
	Tahun	2019
	Judul Artikel	Analisis Penerapan Keamanan Sistem Informasi Pada Pt. AXA Mandiri Financial Service Menggunakan Indeks Kami [30]
	Permasalahan	Keamanan informasi memiliki pedoman yang dapat menjamin kelayakan keamanan informasi suatu instansi, salah satu perusahaan yang telah menerapkan tersebut yaitu PT AXA Mandiri. PT AXA Mandiri merupakan perusahaan *Financial Service,* namun meskipun telah menerapkan Keamanan Informasi masih diperlukan analisis terlebih dahulu untuk mengetahui bagaimana keamanan sistem informasi yang telah diterapkan tersebut.
	Metode	Standar ISO 27001 versi 2013 *Tools* Indeks KAMI Siklus *Plan-Do-Check-Act* (PDCA)

No	Detail Jurnal	
	Hasil dan Kesimpulan	Teknologi dan keamanan informasi pada PT AXA Mandiri *Financial Service* masih membutuhkan penerapan yang lebih baik, karena: a. Tingkat keamanan SMKI PT AXA memiliki perolehan skor yaitu 28, yang berarti PT AXA Mandiri *Financial Service* memiliki ketergantungan. b. Tingkat kematangan PT AXA Mandiri *Financial Service* mendapatkan perolehan skor 249, dimana nilai tersebut berada pada tingkat ke II. Oleh karena itu, dapat disimpulkan bahwa perusahaan terdapat aspek yang masih belum menuju proses penerapan yaitu aspek pengelolaan risiko.
4	Penulis	Yahya Dwi Wijaya
	Jurnal	Jurnal Sistem Informasi dan Informatika (SIMIKA) Vol 4 No 2 Tahun 2021
	Tahun	2021
	Judul Artikel	Evaluasi Keamanan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013 [31]
	Permasalahan	Pasdeal adalah layanan *e-commerce* yang fokus dibidang distributor dan server pulsa. Pasdeal diluncurkan di tahun 2018, dimana sistem informasi Pasdeal belum pernah melakukan evaluasi mengacu pada standar ISO khususnya pada bidang keamanan informasi, sehingga instansi memerlukan analisis terhadap kesiapan instansi dalam mempersiapkan keamanan informasi sesuai dengan standar yang berlaku.
	Metode	Standar ISO 27001 versi 2013 *Tools* Indeks KAMI Siklus *Plan-Do-Check-Act* (PDCA)
	Hasil dan Kesimpulan	Setelah dilakukan evaluasi terhadap sistem informasi Pasdeal, ditemui bahwa Pasdeal mendapatkan tingkat penerapan standar ISO 27001 dengan skor 591, dimana nilai tersebut menunjukan bahwa tingkat penerapan sistem informasi tergolong pada predikat "Baik". Selain itu, sistem informasi Pasdeal berada di tingkat III, dan masih terdapat beberapa jumlah perbaikan.
5	Penulis	Desy Dwi Prasetyowati, Indra Gamayanto, Sasono wibowo, Suharnawi
	Jurnal	Journal of Information System Vol. 4, No. 1, Mei 2019, hlm. 65-75
	Tahun	2019

No	Detail Jurnal	
	Judul Artikel	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang [32]
	Permasalahan	Politeknik Ilmu Pelayaran (PIP) Semarang memiliki keamanan sistem informasi serta jaringan yang masih tergolong lemah dan memiliki dampak yang cukup berbahaya, gangguan tersebut yakni terjadi peretasan pada website PIP Semarang. Peretasan website PIP Semarang pun sudah terjadi sebanyak 2 kali, sehingga PIP Semarang perlu untuk melakukan penilaian keamanan informasi guna untuk meningkatkan kualitas keamanan informasinya.
	Metode	Standar ISO 27001 versi 2013 *Tools* Indeks KAMI Siklus *Plan-Do-Check-Act* (PDCA)
	Hasil dan Kesimpulan	Setelah dilakukan penilaian pada keamanan informasi di Politeknik Ilmu Pelayaran (PIP) Semarang, ditemukan: a. Politeknik Ilmu Pelayaran (PIP) Semarang memiliki nilai 20 untuk tingkat penggunaan sistem elektronik, dimana nilai tersebut tergolong "Tinggi". b. Penilaian kelima area Indeks KAMI pada Politeknik Ilmu Pelayaran (PIP) Semarang mendapatkan skor 238, dimana nilai tersebut menunjukan level I-I+ yang berarti Politeknik Ilmu Pelayaran (PIP) Semarang masih berada pada kategori awal yaitu pada kondisi penerapan keamanan informasi. Sebagai hasilnya, Politeknik Ilmu Pelayaran (PIP) Semarang telah menyadari pentingnya pengelolaan keamanan informasi. Namun demikian, implementasinya masih belum terorganisir dengan baik dan memerlukan perbaikan.

Pada Tabel 2.3 merupakan penelitian terdahulu dengan topik serupa, dari kelima jurnal tersebut memiliki kesamaan dengan penelitian yang dilakukan. Berdasarkan penelitian terdahulu diketahui bahwa banyak sekali perusahaan atau instansi yang belum *aware* akan pentingnya melakukan evaluasi terhadap keamanan informasi dalam perusahaannya, dimana banyak perusahaan mengabaikan dan tidak memikirkan dampak berbahaya yang dapat terjadi [31], [32]. Padahal dengan suatu perusahaan melakukan evaluasi terhadap keamanan informasi maka perusahaan dapat mengetahui kelayakan

keamanan informasi yang diterapkan oleh perusahaannya [30], serta mengetahui ancaman risiko yang dapat terjadi dan bagaimana cara menghindari sebelum terjadinya ancaman tersebut [29]. Maka dari itu, perusahaan perlu untuk melakukan evaluasi keamanan informasi guna untuk melihat kesiapan keamanan informasi di perusahaannya [31]. Salah satu *framework* yang digunakan dalam melakukan evaluasi keamanan informasi suatu instansi atau perusahaan yaitu ISO 27001, evaluasi tersebut juga dapat dibantu dengan *tools* yaitu Indeks KAMI. Indeks KAMI sendiri merupakan alat bantu evaluasi keamanan informasi yang telah disesuaikan dengan standar ISO 27001 versi 2013. Penggunaan *framework* ISO 27001:2013, mengangkat siklus yaitu *Plan-Do-Check-Act* (PDCA). Namun, untuk membantu dalam menyesuaikan kondisi perusahaan maka evaluasi keamanan informasi menggunakan siklus *Check-Act-Plan-Do* (CAPD). Penggunaan siklus tersebut dimulai dari proses *check* yaitu untuk melihat terlebih dahulu kondisi perusahaan saat ini hingga dengan proses *do* yaitu dengan perusahaan melakukan rekomendasi yang telah didapatkan dari hasil evaluasi keamanan informasi dalam perusahaan [12].

Dalam penelitian ini dilakukan evaluasi pada perusahaan, guna mengetahui kesiapan keamanan informasi suatu perusahaan. Dalam evaluasi tersebut tentunya terdapat *framework* yang dijadikan acuan sebagai penilaian yaitu ISO 27001, dengan *tools* Indeks KAMI yang telah disesuaikan dengan standar ISO 27001:2013. Selain itu, adapun siklus yang diadopsi yaitu *Check-Act-Plan-Do* (CAPD). Siklus tersebut diadopsi dalam melakukan evaluasi guna membantu dalam menyesuaikan kondisi perusahaan. Adapun, kebaruan pada penelitian ini dibandingkan pada penelitian sebelumnya yaitu pada objek penelitian dalam mengevaluasi dan rekomendasi Sistem Manajemen Keamanan Informasi. Penelitian ini memiliki objek penelitian yaitu perusahaan yang bergerak di bidang *travel agent*, berbeda dengan penelitian sebelumnya objek penelitiannya merupakan perusahaan atau instansi yang bergerak dibidang lainnya.