BAB II

TINJAUAN PUSTAKA

2.1 Studi Sebelumnya

Studi sebelumnya pada tahun 2020 mengenai evaluasi keamanan informasi menggunakan Indeks KAMI dilakukan oleh Wijatmoko [6]. Penelitian tersebut dilakukan pada Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia (HAM) Daerah Istimewa Yogyakarta. Peneliti dalam penelitian tersebut ingin menggali dan mengevaluasi sejauh mana kesiapan instansi pemerintah dalam hal ini Kantor Wilayah Kementerian Hukum dan HAM DIY untuk menerapkan tata kelola keamanan informasi kemudian akan memberikan rekomendasi terkait dengan keamanan informasi pada Kantor Wilayah Kementerian Hukum dan HAM DIY tersebut.

Penelitian dimulai dengan melakukan studi literatur, wawancara pejabat pengelola dan reviu dokumen, dilanjutkan wawancara mendalam dengan pakar, pengumpulan dan analisis data, dan akhirnya menyusun rekomendasi. Hasil evaluasi pada Kantor Wilayah Kementerian Hukum dan HAM DIY masih belum memenuhi standar yang sudah ditetapkan sesuai dengan ISO 27001. Setelah hasil evaluasi tersebut didapatkan, peneliti memberikan rekomendasi perbaikan untuk meningkatkan penerapan keamanan informasi pada Kantor Wilayah Kementerian Hukum dan HAM DIY kedepannya.

Penelitian lainnya juga dilakukan pada tahun 2020 oleh Ramadhani et al [7]. Penelitian tersebut dilakukan pada Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Malang. Peneliti ingin melakukan evaluasi terkait keamanan informasi menggunakan Indeks KAMI dan memberikan rekomendasi sebagai langkah perbaikan. Penelitian diawali dengan melakukan wawancara kepada pejabat yang bertanggung jawab, dilanjutkan dengan studi literatur, lalu peneliti menyebarkan kuesioner kepada responden yang sudah terpilih, validasi data kuesioner, analisis data hasil kuesioner, dan diakhiri dengan penyusunan kesimpulan dari evaluasi tersebut. Hasil dari evaluasi tersebut menunjukkan bahwa Diskominfo Kabupaten Malang belum memenuhi standar penerapan ISO

27001. Rekomendasi yang diberikan oleh peneliti mencakup seluruh area pengevaluasian [7].

Penelitian lainnya dilakukan pada tahun 2020 oleh Rahmah et al [2]. Penelitian tersebut dilakukan pada Diskominfo Kabupaten Mojokerto. Peneliti melakukan penelitian tersebut dengan maksud untuk mendapatkan penilaian pengelolaan keamanan informasi, tingkat kematangan, dan menyusun rekomendasi berdasarkan hasil analisis pengelolaan keamanan informasi pada Diskominfo Kabupaten Mojokerto dengan menggunakan standar ISO 27001. Penelitian diawali dengan perencanaan penelitian berdasarkan studi literatur, menentukan rencana penelitian berdasarkan Indeks KAMI, penyebaran kuesioner kepada responden yang terpilih dan mengumpulkan kuesioner tersebut, data diolah ke dalam format Indeks KAMI, konfirmasi data, analisis data menggunakan Indeks KAMI, kemudian *checklist* hasil evaluasi dengan standar ISO 27001. Berdasarkan hasil evaluasi yang didapatkan, tingkat kesiapan keamanan informasi Diskominfo Kabupaten Mojokerto masih rendah dan belum memenuhi syarat. Peneliti memberikan rekomendasi pada seluruh bagian area yang dievaluasi [2].

Penjelasan tentang penelitian-penelitian sebelumnya yang akan disajikan secara ringkas pada Tabel 2.1 berikut ini.

Tabel 2.1 Ringkasan Penelitian Sebelumnya

No	Nama Penulis	Tahun	Tujuan	Metode	Hasil
1	Wijatmoko [6]	2020	Untuk menggali dan mengevaluasi sejauh mana kesiapan Kantor Wilayah Kementerian Hukum dan HAM DIY untuk menerapkan tata kelola keamanan informasi kemudian akan memberikan rekomendasi terkait dengan keamanan informasi.	Indeks KAMI	Berdasarkan hasil evaluasi pada Kantor Wilayah Kementerian Hukum dan HAM DIY masih belum memenuhi standar yang sudah ditetapkan sesuai dengan ISO 27001. Peneliti memberikan rekomendasi perbaikan untuk meningkatkan penerapan keamanan informasi.

2	Ramadhani et al.[7]	2020	Melakukan evaluasi terkait keamanan informasi menggunakan Indeks KAMI dan memberikan rekomendasi sebagai langkah perbaikan.	Indeks KAMI	Hasil evaluasi menunjukkan bahwa Diskominfo Kabupaten Malang belum memenuhi standar penerapan ISO 27001. Peneliti memberikan rekomendasi yang mencakup seluruh area pengevaluasian.
3	Rahmah et al.[2]	2020	Untuk mendapatkan penilaian pengelolaan keamanan informasi, mengetahui tingkat kematangan, dan menyusun rekomendasi berdasarkan hasil analisis pengelolaan keamanan informasi pada Dinas Komunikasi Informasi Kabupaten Mojokerto dengan menggunakan standar ISO 27001	Indeks KAMI	Berdasarkan hasil evaluasi yang didapatkan, tingkat kesiapan keamanan informasi Diskominfo Kabupaten Mojokerto masih rendah dan belum memenuhi syarat. Peneliti memberikan rekomendasi pada seluruh bagian area yang dievaluasi.

Dapat dilihat dari Tabel 2.1, bahwa dari penelitian sebelumnya menilai evaluasi keamanan informasi menggunakan Indeks KAMI 4.1, sedangkan pada penelitian ini evaluasi keamanan informasi tersebut dinilai menggunakan Indeks KAMI 4.2. Perubahan versi dari Indeks KAMI 4.1 menjadi 4.2 tersebut dikarenakan ada formulasi yang tidak sesuai pada Indeks KAMI 4.1. Perbedaan kedua versi Indeks KAMI tersebut akan dijelaskan pada Sub-bab 2.3.

2.2 Dasar Teori

2.2.1 Keamanan Informasi

Meskipun konsep keamanan informasi menjadi lebih populer setelah diperkenalkannya komputer dalam kehidupan kita, informasi telah digunakan sejak dahulu kala sebagai nilai sosial dan ekonomi. Kerahasiaan informasi dan komunikasi antara para raja, pemimpin, dan politisi pada zaman dahulu kala sudah dilindungi dengan alat pengamanan berupa segel, lem khusus, pengkodean dan kotak terkunci. Lalu dikarenakan penemuan Listrik selama

revolusi industri, pengembangan dan penyebaran teknologi komunikasi menjadi semakin maju dan luas, sehingga menghasilkan terobosan dalam keamanan informasi pada sektor komunikasi dengan sinyal, suara dan gambar yang dibawa melalui arus listrik maupun gelombang frekuensi tertentu. Dengan penyebarluasan penggunaan internet yang terjadi pada tahun 1990-an, bahaya yang menargetkan sistem informasi mulai bermunculan dimana-mana [8].

Banyak organisasi yang menemukan sisi komersial dari internet yang terlibat dalam persaingan ketat untuk mendapatkan keuntungan maksimum dari hal tersebut. Efek sampingnya adalah inovasi sistem informasi yang sangat cepat berkembang dan transisi ke tahap baru untuk memanfaatkan hal tersebut secara maksimal. Namun, pengembangan dan modernisasi dari sistem informasi maupun aplikasi dengan pendekatan modern tidak diikuti oleh modernisasi keamanan informasi, dan kebanyakan tingkat keamanan dari sistem informasi maupun aplikasi tersebut diabaikan sebagai hasil dari periode pengembangan yang tidak sesuai dengan prinsip-prinsip utama keamanan informasi yaitu *Confidentiality*, *Integrity* dan *Availability* (CIA) [8].

Oleh karena itu saat ini keamanan Informasi merupakan suatu upaya untuk mencegah agar aset informasi aman dari berbagai macam ancaman yang dapat terjadi untuk meminimalisir risiko negatif yang diterima [9]. Sebelumnya telah disebutkan bahwa keamanan informasi terdiri dari 3 aspek, yaitu *Confidentiality*, *Integrity*, dan *Availability* (CIA). *Confidentiality* (kerahasiaan) merupakan aspek keamanan informasi yang menjamin bahwa data dan informasi hanya dapat diakses oleh pihak yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan. *Integrity* (integritas) merupakan aspek keamanan informasi yang menjamin bahwa data tidak dapat dirubah tanpa izin pihak yang berwenang, keakuratan dan keutuhan sebuah informasi harus terjaga. *Availability* (ketersediaan) merupakan aspek keamanan informasi yang menjamin bahwa data dan informasi akan tersedia kapanpun untuk diakses oleh pengguna yang memiliki hak akses [10].

Saat ini, penggunaan Teknologi Informasi dan Komunikasi (TIK) di instansi pemerintahan terus berkembang, seiring dengan kebutuhan untuk menyediakan layanan publik yang cepat, handal, dan aman sesuai dengan prinsip-prinsip

keamanan informasi seperti Konfidensialitas, Integritas, dan Ketersediaan (CIA). Hal ini mengakibatkan munculnya potensi kerentanan dan ancaman terhadap keamanan informasi, yang bisa mengganggu efektivitas penyelenggaraan layanan publik. Kementerian Komunikasi dan Informatika telah mengimbau kepada seluruh instansi pemerintah, terutama yang bertanggung jawab atas layanan publik dan yang memiliki infrastruktur krusial, untuk meningkatkan kesadaran tentang pentingnya keamanan informasi.

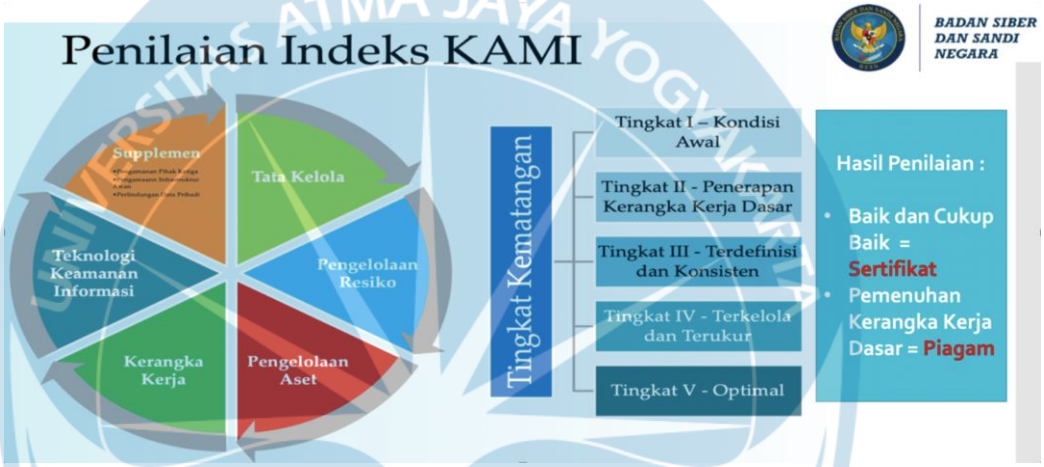
Sistem Manajemen Keamanan Informasi (SMKI) yang telah diperkenalkan oleh *International Standards Organization* (ISO) dalam bentuk standar ISO/IEC 27001 merupakan salah satu upaya dalam menstandarisasi pengamanan informasi dengan menggunakan pelaksanaan analisis risiko sebagai landasan strategi keamanan informasi dimana situasi risiko baru diidentifikasi dan dengan begitu maka tindakan mitigasi yang sesuai dapat dilakukan [11]. Kementerian Komunikasi dan Informatika, bersama dengan Badan Siber dan Sandi Negara, telah mengadopsi standar keamanan informasi dari ISO/ IEC 27001 dalam bentuk SNI ISO/ IEC 27001. Badan Siber dan Sandi Negara juga telah menciptakan Indeks Keamanan Informasi (KAMI) sebagai alat untuk mengukur tingkat implementasi keamanan informasi di instansi pemerintahan.

2.2.2 Indeks Keamanan Informasi (KAMI)

Indeks Keamanan Informasi (KAMI) adalah sebuah alat yang menggabungkan berbagai aspek pengamanan informasi untuk mengevaluasi status terkini pengamanan informasi dan tingkat kematangan program keamanan informasi yang diterapkan oleh suatu organisasi [12]. Indeks KAMI berfungsi sebagai alat yang digunakan untuk menilai tingkat kematangan dan kelengkapan penerapan standar ISO/IEC 27001:2013, serta memberikan gambaran tentang tata kelola keamanan informasi dalam organisasi tersebut [13]. Tujuan dibuatnya Indeks KAMI adalah untuk memungkinkan organisasi, baik pada tingkat nasional maupun yang lebih kecil, untuk menilai dan membandingkan kondisi keamanan informasi mereka, mengidentifikasi area perbaikan, dan menetapkan prioritas. Evaluasi menggunakan Indeks KAMI ini sebaiknya dilakukan secara rutin oleh

pejabat yang memiliki tanggung jawab dalam pengelolaan keamanan informasi di seluruh bagian organisasi.

Dalam konteks instansi pemerintahan, penggunaan Indeks KAMI penting untuk menjalankan evaluasi tahunan yang diwajibkan. Penggunaan KAMI oleh instansi pemerintah juga dapat membantu meningkatkan tingkat keamanan informasi mereka. Penilaian dalam Indeks KAMI dilakukan dengan mengevaluasi semua persyaratan keamanan yang dijelaskan dalam standar ISO/IEC 27001:2013, yang telah diorganisir menjadi enam area seperti yang ditampilkan pada Gambar 2.1 [14] berikut:



Gambar 2.1 Penilaian Indeks KAMI

1. Tata Kelola Keamanan Informasi

Pada area ini pengevaluasian dilakukan untuk menilai kesiapan bentuk tata kelola keamanan informasi beserta fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Di area ini juga terdapat hal-hal krusial seperti *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP).

a. *Business Continuity Plan* (BCP)

BCP adalah suatu proses yang disusun dengan tujuan mengurangi potensi ancaman terhadap fungsi-fungsi penting organisasi serta memastikan kelangsungan layanan untuk operasi yang vital. BCP dibuat untuk melindungi operasi bisnis yang krusial dari dampak bencana, kesalahan manusia, atau kerusakan yang bisa terjadi, dan dampak kerugian yang mungkin terjadi jika operasi bisnis tidak berjalan sebagaimana mestinya adalah hal yang biasa [15].

Keberadaan BCP memiliki peran yang sangat penting dalam menjaga kelangsungan bisnis.

b. *Disaster Recovery Plan* (DRP)

DRP adalah suatu strategi pemulihan kinerja yang bertujuan untuk memastikan ketersediaan kemampuan dan sumber daya yang diperlukan dalam menjalankan operasi bisnis yang krusial di lokasi cadangan, yang dikenal sebagai *Disaster Recovery Center* (DRC). Perencanaan DRP ini memiliki kepentingan yang sangat besar untuk memastikan kelangsungan operasional bisnis yang vital ketika terjadi bencana serta untuk mengurangi risiko yang tidak dapat diterima oleh organisasi tersebut [12].

2. Pengelolaan Risiko Keamanan Informasi

Pengevaluasian pada area ini dilakukan untuk menilai kesiapan penerapan pengelolaan risiko keamanan informasi sebagai landasan strategi keamanan informasi.

3. Kerangka Kerja Keamanan Informasi

Pengevaluasian pada area ini dilakukan untuk menilai kecukupan dan kesiapan kerangka kerja manajemen keamanan informasi serta strategi penerapannya.

4. Pengelolaan Aset Informasi

Pengevaluasian pada area ini dilakukan untuk menilai kecukupan perlindungan terhadap aset informasi, termasuk seluruh siklus penggunannya.

5. Teknologi dan Keamanan Informasi

Pengevaluasian pada area ini dilakukan untuk menilai kecukupan, konsistensi, dan efektivitas penggunaan teknologi dalam mengamankan aset informasi.

2.2.3 Penilaian dalam Indeks KAMI

Sebelum mengevaluasi, terlebih dahulu dilakukan pengklasifikasian terhadap kategori Sistem Elektronik. Pemilihan kategori Sistem Elektronik ini bertujuan untuk mengategorikan instansi ke dalam tingkat tertentu [6]. Kategori sistem elektronik ini terdiri dari tiga tingkat, yaitu rendah, tinggi, dan strategis yang dapat dilihat pada Tabel 2.2 Contoh Kategori Sistem Elektronik pada Indeks KAMI[14] berikut ini:

Tabel 2.2 Contoh Kategori Sistem Elektronik pada Indeks KAMI

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	B
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

Pertanyaan dalam Indeks KAMI dibagi menjadi dua kategori berdasarkan kebutuhan. Pertama, pertanyaan diklasifikasikan berdasarkan tingkat kesiapan implementasi keamanan sesuai dengan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Dalam kategori ini, responden diminta memberikan tanggapan tentang tiga aspek: kerangka kerja dasar keamanan informasi (ditandai sebagai "1"), efektivitas dan konsistensi implementasinya (ditandai sebagai "2"), serta kemampuan untuk terus meningkatkan kinerja keamanan informasi (ditandai sebagai "3"). Tingkat terakhir ini sesuai dengan kesiapan minimum yang dibutuhkan untuk proses sertifikasi standar ISO/IEC 27001.

Setiap jawaban akan dinilai dengan skor yang nantinya akan diolah untuk menghasilkan indeks, dan hasil evaluasi akan ditampilkan dalam *dashboard* pada akhir proses ini. Skor yang diberikan untuk setiap jawaban akan sesuai dengan tingkat kematangannya, seperti yang tercantum dalam Tabel 2.3 [14] berikut:

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

Hasil evaluasi untuk setiap area akan direpresentasikan dalam diagram radar yang menampilkan tingkat kematangan dari 1 hingga 3. Diagram ini memungkinkan perbandingan kondisi kesiapan dari evaluasi dengan tingkat kematangan yang telah ditetapkan sebagai acuan.

Dengan mengamati diagram tersebut, para pimpinan instansi dapat mengidentifikasi kebutuhan perbaikan yang diperlukan dan hubungan antara berbagai area penerapan keamanan informasi. Korelasi antara Kategori Sistem Elektronik dan Status Kesiapan dijelaskan lebih lanjut dalam Tabel 2.4 [14] berikut:

Tabel 2.4 Matriks Kategori Sistem Elektronik dan Status Kesiapan

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

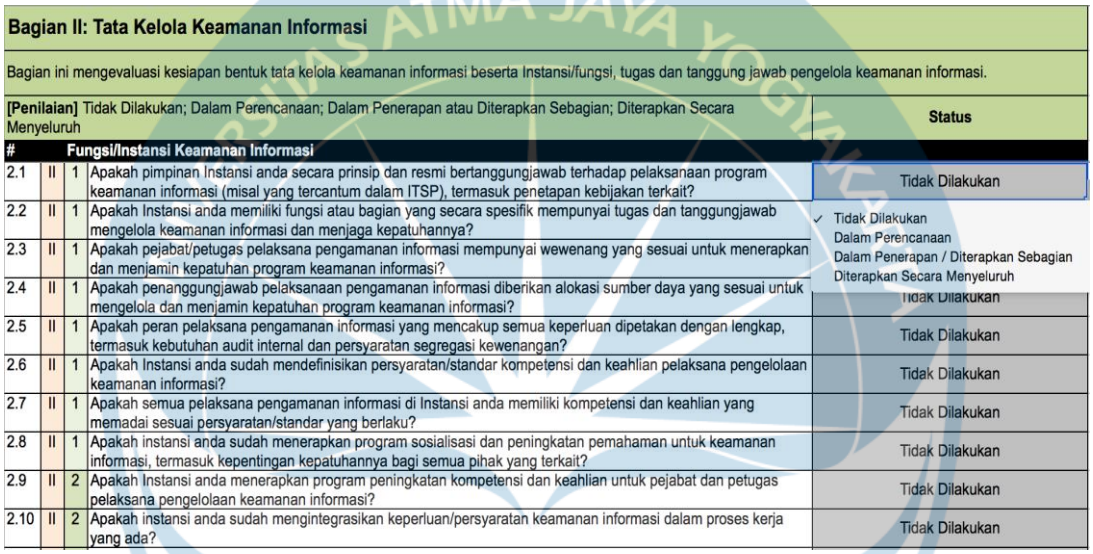
Pengelompokkan kedua dilakukan berdasarkan tingkat kematangan implementasi keamanan dengan kategori yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini akan digunakan sebagai sarana untuk melaporkan pemetaan dan peringkat kesiapan keamanan informasi di Kementerian/ Lembaga.

Dalam Indeks KAMI, tingkat kematangan ini didefinisikan sebagai berikut:

1. Tingkat I – Kondisi Awal

2. Tingkat II – Penerapan Kerangka Kerja Dasar
3. Tingkat III – Tedefinisi dan Konsisten
4. Tingkat IV – Terkelola dan Terukur
5. Tingkat V - Optimal

Untuk memberikan penjelasan yang lebih rinci, tingkatan ini diperluas dengan tambahan tingkatan I+, II+, III+, dan IV+, sehingga secara total ada 9 tingkatan kematangan. Awalnya, semua responden akan diberikan kategori kematangan pada Tingkat I, Sebagai standar yang setara dengan ISO/IEC 27001:2013, tingkat kematangan yang diinginkan untuk standar minimum sertifikasi adalah tingkat III+.



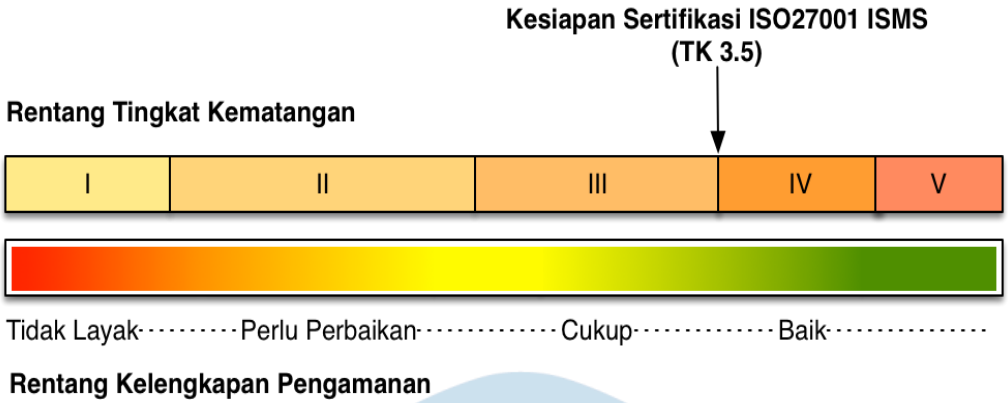
Bagian II: Tata Kelola Keamanan Informasi

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
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan
2.8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Tidak Dilakukan

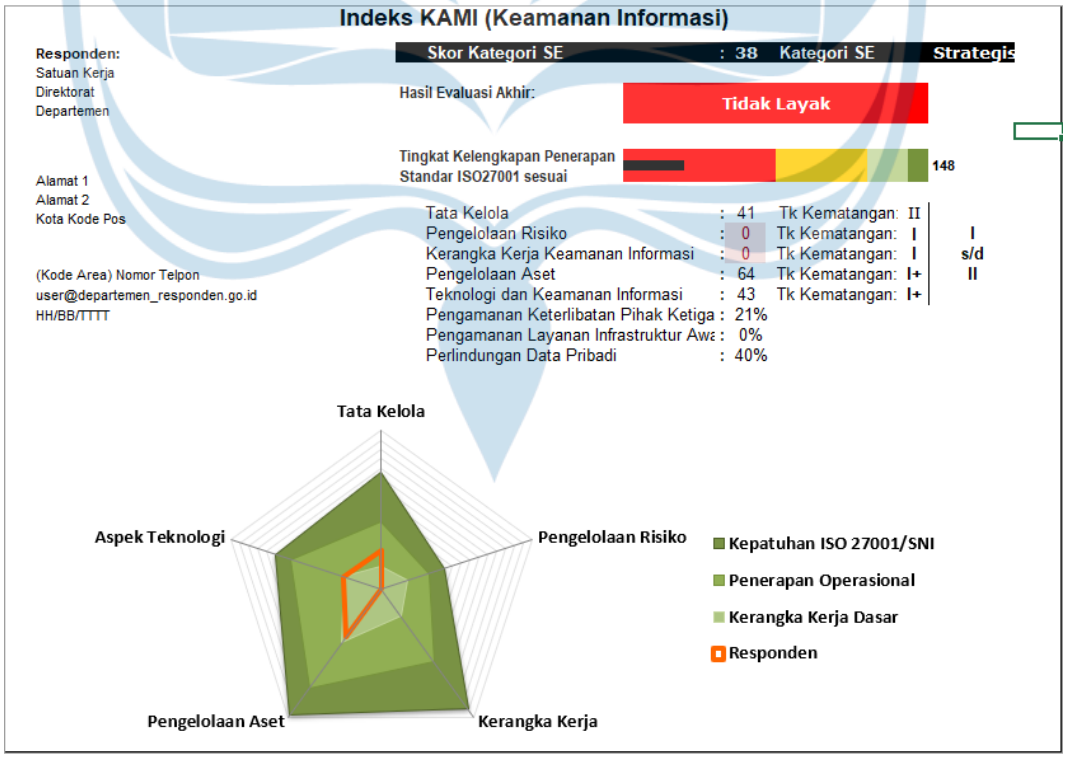
Gambar 2.2 Contoh Pertanyaan pada Indeks KAMI

Kedua Pengelompokkan ini dapat dipetakan untuk memberikan dua sudut pandang yang berbeda yaitu dari sudut pandang tingkat kelengkapan keamanan dan tingkat kematangan pengamanan. Pengelompokkan yang dipetakan tersebut dapat dilihat pada Gambar 2.3 [14] di bawah ini.



Gambar 2.3 Rentang Tingkat Kematangan

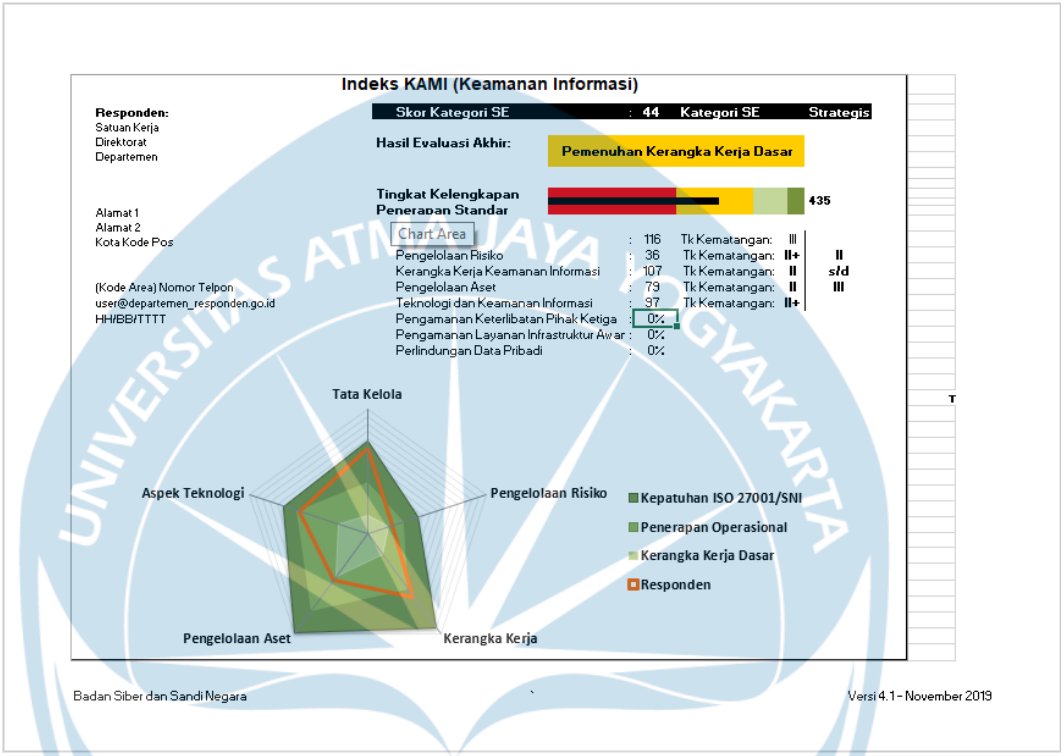
Hasil evaluasi dari Indeks KAMI versi 4.2 akan ditampilkan ke dalam sebuah diagram yang berbentuk seperti jaring laba-laba (*spider chart*) dengan 6 area utama. Diagram tersebut juga akan menunjukkan tentang nilai Indeks KAMI dengan kepatuhan terhadap ISO 27001:2013. Contoh skor akhir yang disesuaikan dengan status kesiapan dari instansi terkait mengenai keamanan informasinya dapat dilihat pada Gambar 2.4 [14] berikut.



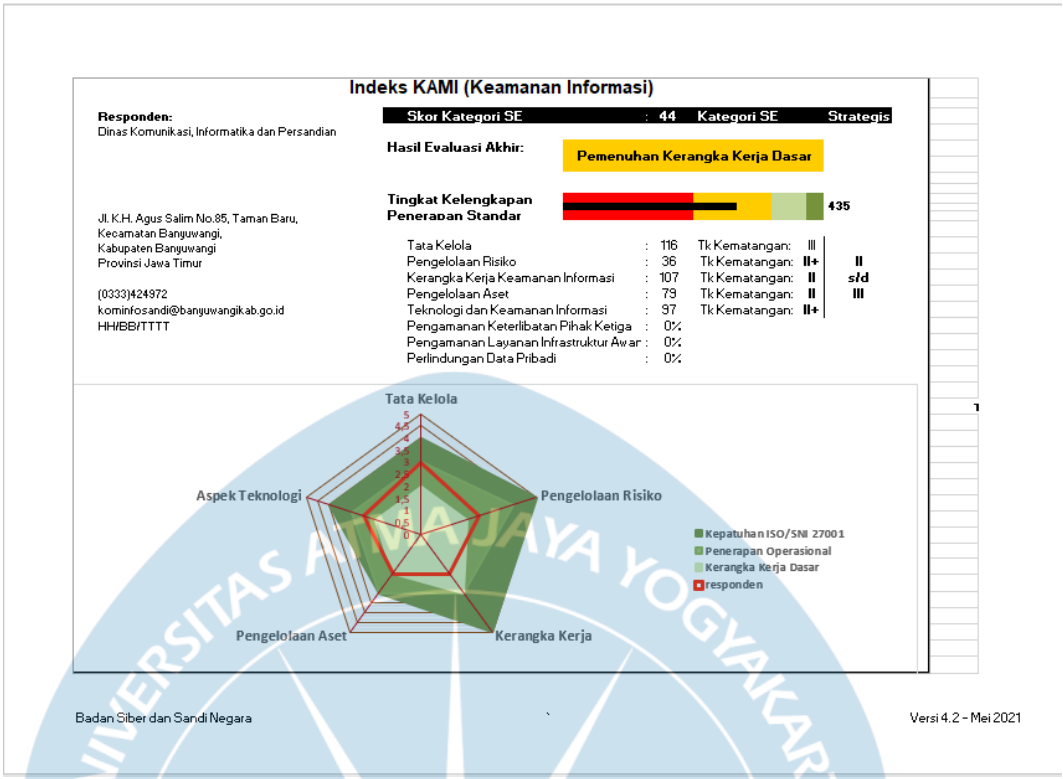
Gambar 2.4 Contoh Dashboard Hasil Evaluasi Indeks KAMI

2.3 Perbedaan Indeks Keamanan Informasi (KAMI) Versi 4.1 dan Versi 4.2

Sebelumnya telah disebutkan bahwa pada Indeks KAMI Versi 4.1 memiliki kesalahan formulasi pada *sheet dashboard*. Hal tersebut dapat dilihat dengan membandingkan hasil pada Gambar 2.5 [14] dan Gambar 2.6 [14] yang programnya sudah diisi dengan nilai yang sama berikut.



Gambar 2.5 Dashboard Indeks KAMI Versi 4.1



Gambar 2.6 Dashboard Indeks KAMI Versi 4.2

Berdasarkan Gambar 2.5 [14] dan Gambar 2.6 [14], dapat dilihat perbedaan yang signifikan pada *chart* jaring laba-laba. Pada Gambar 2.6 [14] kita dapat melihat nilai maksimal tingkat kematangan dari masing-masing aspek Indeks KAMI yang tidak dapat kita lihat pada Gambar 2.5 [14] dan juga nilai maksimal tingkat kematangan pada Gambar 2.5 [14] belum sesuai dengan nilai maksimal tingkat kematangan yang sudah ditetapkan pada masing-masing aspek yang ada dalam Indeks KAMI. Aspek-aspek yang dimaksud adalah Pengelolaan Risiko Keamanan Informasi dan Pengelolaan Aset Informasi.