BAB II
TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Penelitian sebelumnya yang dilakukan oleh Darmanto dkk [12] melakukan analisis tingkat kesiapan keamanan informasi menggunakan Indeks KAMI versi 4.2 yang dilakukan pada Politeknik Negeri Ketapang. Tujuan dari penelitian ini adalah untuk mendapatkan gambaran terkait keamanan informasi dan memberikan rekomendasi perbaikan. Penelitian dilakukan dalam bentuk deskriptif kualitatif yang dimulai dengan wawancara dan observasi, pengumpulan data dengan menggunakan kuesioner yang sudah disediakan oleh Indeks KAMI 4.2, analisis data yang mana untuk memastikan validitas, dan yang terakhir memberikan kesimpulan dan saran. Hasil dari penelitian dari Politeknik Negeri Ketapang menggunakan Indeks KAMI versi 4.2 yaitu berada di level II – II+ dengan Pemenuhan Kerangka Kerja Dasar. Dengan berada di tingkat kematangan level II – II+, perlu adanya perbaikan dalam pengamanan dan pengawasan, serta meningkatkan kesadaran tanggung jawab dari pihak berwenang.

Penelitian selanjutnya dilakukan oleh Bakhtiar & Hidayat [13] dengan melakukan penelitian di Provinsi Jawa Tengan pada Dinas XYZ. Tujuan dari dilakukannya penelitian ini yaitu mengukur level kesiapan dan juga kematangan sistem manajemen keamanan informasi yang telah diterapkan oleh Dinas XYZ dengan menggunakan indeks KAMI versi 4.2. Metode yang digunakan berupa deskriptif kuantitatif dengan mengumpulkan data dengan wawancara, observasi, dan dokumentasi. Perolehan hasil yang didapat yaitu total skor keseluruhan 225 yang tergolong “Tidak Layak”. Penilaian Tata Kelola Keamanan Informasi memperoleh skor 43 dengan tingkat kematangan I+, pengelolaan risiko keamanan mendapatkan skor 34 di tingkat kematangan II, Kerangka Kerja Keamanan Informasi dengan skor 44 dengan tingkat kematangan I+, dan Teknologi dan Keamanan Informasi mendapatkan skor 53 dengan tingkat kematangan. Penilaian pada suplemen mendapatkan 36% dengan keterlibatan

pihak ke 3, lalu mendapatkan 33% di pengamanan layanan infrastruktur awan, dan yang terakhir mendapatkan 38% di bagian perlindungan data pribadi.

Penelitian berikutnya dilakukan oleh Wijatmoko [14] dengan mengevaluasi bagian keamanan informasi di Kantor Wilayah Kementerian Hukum dan HAM DIY menggunakan Indeks KAMI versi 4.1. Penelitian yang dilakukan oleh Wijatmoko digunakan untuk menggali, mengevaluasi dan memberikan sebuah rekomendasi yang berhubungan dengan keadaan di kantor Wilayah Kementerian Hukum dan HAM DIY. Metode yang digunakan yaitu metode kualitatif dengan melakukan 3 tahap yaitu, tahap 1 mengidentifikasi masalah dan tinjauan literatur, tahap ke-2 yaitu analisis data dan pengumumpulan data, dan tahap ke-3 melakukan rekomendasi.

Hasil yang diperoleh dari penelitian menggunakan Indeks KAMI versi 4.1 mendapatkan skor 314 dari total skor keseleruhan 645 dengan berada di tingkat II yaitu Penerapan Kerangka Kerja Dasar. Pada bagian kategori Sistem Elektronik mendapatkan skor sebesar 32 dari totsl 50 yang artinya Kantor HAM DIY tinggi dalam penggunaan *e-government*. Selain itu tingkat kematangan area lainnya yaitu area Tata Kelola Keamana informasi di tingkat II dengan skor 69, area Pengelolaan Risiko Keamanan Informasi di tingkat I+ mendapatkan skor 31, area Kerangka Kerja Pengelolaan Keamanan Informasi di tingkat I+ mendapatkan skor 47, area Pengelolaan Aset Informasi di tingkat II mendapatkan skor 89, dan Teknologi dan Keamanan Informasi di tingkat II dengan skor 76.

Selanjutnya penelitian yang diteliti oleh Firdani dkk [15] yang bertujuan untuk memberikan rancangan terkait dengan keaman informasi berdasarkan analisis risiko pada Diskominfo Kabupaten Rembang. Metode yang digunakan yaitu mengidentifikasi permaslahan dengan wawancara kepada karyawan yang memiliki tugas dan tanggung jawab. Untuk menghitung nilai risiko menggunakan metode FMEA yang menjadi acuan pemilihan dalam pengendalian risiko. Lalu di lanjutkan dengan pengumpulan data dengan studi lapangan dan membagikan kuesioner kepada karyawan yang memiliki tugas dan tanggung jawab. Selanjutnya, menganalisis dengan menerapkan ISO 27001

yang berdasarkan hasil kuesioner Indeks KAMI. Dengan penelitian ini mendapatkan hasil kelengkapan skor 161 dengan mendapatkan level "Tidak Layak". Dengan hasil skor yang sudah diperoleh dari kelima area keamanan informasi mendapatkan di level I sampai dengan I+ yang artinya masih di kondisi awal. Dengan nilai tertinggi di area teknologi dan Keamanan Informasi yang mendapatkan skor 43 dan mendapatkan nilai terendah dengan skor 17 berada di area pengelolaan Risiko.

Penelitian terakhir dilakukan oleh Yuliani, dkk [16] menggunakan Indeks KAMI yang bertujuan untuk mengukur dan analisis tingkat kematangan dalam pengamanan informasi. Penelitian ini dilakukan di PT. Telekomunikasi Indonesia (TELKOM). Dalam penelitian ini menggunakan metode kualitatif murni yang mana hasil dari penelitian ini untuk mendeskripsikan hasil yang sudah diteliti. Dengan menggunakan metode ini dapat mengeksplor objek dengan prosedur wawancara bersama pihak yang terkait. Lalu untuk Teknik pengumpulan data dengan teknik tringulasi yang isinya wawancara, observasi dan dokumentasi. Untuk *tools* yang digunakan dalam penelitian ini menggunakan wawancara, *work paper*, kamera, dan lainnya. Selain itu, mekanisme analisis di penelitian ini dilakukan dengan cara analisis untuk *maturity*, yang akan digunakan untuk perbandingan tingkat *maturity* sekarang dengan *maturity* yang disetujui [16].

Dalam penelitian ini, PT. TELKOM mendapatkan hasil di level "Baik" dengan skor 597 dari 645 skor maksimum yang artinya PT. TELKOM termasuk tergolong baik untuk keamanan informasinya serta telah memenuhi standar ISO 27001 yang baik. Hasil dari setiap area Tata Kelola mendapatkan nilai 116 dengan tingkat keamanan mencapai II+, skor di area Pengelolaan Risiko mendapatkan nilai 72 dengan tingkat keamananan mencapai V. Area Kerangka Kerja Keamanan Informasi mendapatkan nilai 159 dengan mencapai tingkat keamanan V, lalu area yang terakhir yaitu Pengelolaan Aset Informasi mempunyai nilai 150 dengan mencapai tingkat keamanan III [16].

Tabel 2. 1. Studi Sebelumnya

NO	Penulis	Tahun	Tujuan	Pendekatan	Alat	Hasil
1.	Darmanto, dkk [12]	2024	Tujuan dari penelitian ini adalah untuk mendapatkan gambaran terkait keamanan informasi dan memberikan rekomendasi perbaikan.	Kualitatif	Indeks KAMI versi 4.2	Hasil yang diperoleh dari penelitian ini yaitu berada di level II – II+ pada status Pemenuhan Kerangka Kerja Dasar. Dengan di level II – II+, perlu adanya perbaikan dalam pengamanan dan pengawasan, serta meningkatkan kesadaran tanggung jawab dari pihak berwenang.
2.	Bakhtiar & Hidayat [13]	2023	Mengukur level kesiapan dan kematangan SMKI yang diterapkan oleh Dinas XYZ.	Deskriptif kuantitatif	Indeks KAMI versi 4.2	total skor keseluruhan 225 yang tergolong "Tidak Layak". Hasil setiap area dari tata Kelola mendapatkan 43 di tingkat kematangan I+, skor 34 dengan tingkat kematangan II pada risiko keamanan, kerangka kerja dengan hasil 44 di tingkat kematangan I+, dan untuk teknologi memperoleh 53 dengan tingkat kematangan I. Tambahan penialain yaitu suplemen yang didalamya ada keterlibatan pihak ketiga 36%, pengamanan layanan infrastruktur (*Cloud*) 33%, dan perlindungan data pribadi mendapatkan 38%. Hasil yang didapat artinya Dinas XYZ belum menyentuh ambang batas kesiapan ISO 27001.
3.	Wijatmoko [14]	2020	Menggali evaluasi dan memberikan rekomendasi yang sesuai dengan keaadaan di Kantor Wilayah Kementerian Hukum dan HAM DIY.	Kualitatif	Indeks KAMI versi 4.1	mendapatkan skor 314 dari total skor keseleruhan 645 dengan berada di tingkat II yaitu Penerapan Kerangka Kerja Dasar. Pada bagian kategori Sistem Elektronik mendapatkan skor sebesar 32 dari total 50 yang artinya tinggi dalam penggunaan *e-government*. Selain itu tingkat kematangan area lainnya yaitu area Tata

NO	Penulis	Tahun	Tujuan	Pendekatan	Alat	Hasil
						Kelola Keamana informasi di tingkat II dengan skor 69, area Pengelolaan Risiko Keamanan Informasi di tingkat I+ mendapatkan skor 31, area Kerangka Kerja Pengelolaan Keamanan Informasi di tingkat I+ mendapatkan skor 47, area Pengelolaan Aset Informasi di tingkat II mendapatkan skor 89, dan area Teknologi dan Keamanan Informasi di tingkat II dengan skor 76.
4.	Firdan, dkk [15]	2019	untuk memberikan rancangan terkait dengan keaman informasi berdasarkan analisis risiko pada Diskominfo Kabupaten Rembang.	Kualitatif dan FMEA untuk menghitung nilai risiko	Indeks KAMI	penelitian ini mendapatkan hasil kelengkapan skor 161 dengan mendapatkan level "Tidak Layak". Dengan hasil skor yang sudah diperoleh dari kelima area keamanan informasi mendapatkan di level I sampai dengan I+ yang artinya masih di kondisi awal. dilihat nilai tertinggi ada pada area teknologi dan Keamanan Informasi yang mendapatkan skor 43 dan mendapatkan nilai terendah dengan skor 17 berada di area pengelolaan Risiko
5.	Yuliani, dkk [16]	2020	untuk mengukur dan analisis tingkat kematangan dalam pengamanan informasi. Penelitian ini dilakukan di PT. Telekomunikasi Indonesia (TELKOM).	Kualitatif Murni	Indeks KAMI	Dalam penelitian ini memperoleh hasil di level "Baik" dengan skor 597 dari 645 skor maksimum yang artinya PT. TELKOM tergolong baik untuk keamanan informasinya dan telah mencapai standar ISO 27001 yang baik. Hasil dari setiap area Tata Kelola mendapatkan nilai 116 dengan tingkat keamana mencapai II+, skor di area Pengelolaan Risiko mendapatkan nilai 72 dengan tingkat keamananan mencapai V. Area Kerangka Kerja Keamanan Informasi mendapatkan nilai

NO	Penulis	Tahun	Tujuan	Pendekatan	Alat	Hasil
						159 dengan mencapai tingkat keamanan V, lalu area yang terakhir yaitu Pengelolaan Aset Informasi mempunyai nilai 150 dengan mencapai tingkat keamanan III

2.2. Dasar Teori

2.2.1. Kemanan informasi

Keamanan informasi sendiri merupakan sebuah upaya yang dilakukan untuk menjaga keamanan data dari ancaman yang datang dari berbagai macam dan memastikan proses bisnis yang berlangsung dari instansi pemerintah, perusahaan swasta, dan organisasi. Dengan adanya keamanan informasi dapat mengurangi resiko kerusakan yang mungkin terjadinya akibat ancaman yang muncul [17]. Secara tidak langsung, keamanan informasi dapat menjamin keberlanjutan proses bisnis, menekan seluruh resiko yang ada, dan bisa memaksimalkan nilai investasi.

Keamanan informasi juga sebagai aspek utama dalam menjaga aset-aset informasi di suatu organisasi, instansi pemerintah, perusahaan maupun organisasi. Untuk mengukur keamanan informasi selain menggunakan Indeks KAMI yaitu ada *COBIT, OCTAVE*, *Nist Cybersecurity Framework (CSF)*, *ITIL,* dll [18]. Keamanan informasi dapat memiliki beberapa jenis-jenis keamanan informasi yang dapat dikelompokkan sebagai berikut [4]**:**

1. *Application Security,* mengarah terhadap kerentanan perangkat lunak seperti di *aplikasi mobile* dan *Application program interface* (APIs), terutama pada proses otentikasi, integritas kode, dan kebijakan pengguna.
2. *Cloud Security* adalah teknologi, prosedur, kebijakan, dan kontrol dan *hosting* keamanan aplikasi yang berbasis *cloud* atau melindungi sistem dan data berbasis *cloud,* termasuk melibatkan dengan pihak ketiga. Bisnis juga perlu memastikan adanya isolasi yang membagi proses lingkungan eksternal dengan lingkungan internal, untuk menjaga tingkat keamanan data yang diakses.
3. *Infrastructure Security,* merupakan prakter untuk melindungi sistem dan aset kritis dari ancaman *cyber* dan fisik. Perlindungan yang diberikan bisa dari internal dan eksternal, laboratorium, *data center*, *server*, dan perangkat lainnya yang berhubungan.

4. *Incident Response* adalah fungsi untuk memonitor terkait perilaku yang berbahaya bagi data atau aset digital perusahaan. Untuk mengatasi hal tersebut maka diperlunya staf IT memiliki rencana *incident response* yang dapat digunakan untuk menyimpan bukti dan dijadikan bahan evaluasi untuk ke depannya.
5. *Vulnerability Management* proses pencarian kerentanan untuk mengidentifikasi dan memperbaiki kelemahan sistem, aplikasi, dan infrastruktur sebelum terserang *malware*. Dengan adanya celah, maka bisa dilakukan adanya perbaikan dan pengecekan terhadap kerentanan yang kemungkinan sebuah bisnis untuk selalu menambahkan aplikasi, pengguna, dan infrastruktur.

2.2.2. Indeks KAMI versi 4.2

Indeks KAMI merupakan sebuah alat yang bisa digunakan guna menilai, evaluasi suatu tingkat kematangan dan kelengkapan penerapan ISO 27001, sekaligus pemetaan setiap area tata kelola keamanan sistem informasi di suatu instansi pemerintah, perusahaan, maupun organisasi. Alat ini disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika. Indeks KAMI tidak dimaksudkan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada termasuk teknologi yang digunakan pada suatu instansi, perusahaan maupun organisasi. Melainkan digunakan sebagai alat evaluasi untuk memberikan gambaran mengenai kondisi kesiapan kerangka kerja keamanan informasi [19][20]. Evaluasi dilakukan dengan cara melihat hasil yang telah di peroleh melalui jawaban responden. Sedangkan gambaran di setiap area di dapat berdasarkan hasil dari pengolahan data Indeks KAMI yang nantinya akan ditampilkan pada *dashboard*. Tampilan *dashboard* dapat dilihat pada Gambar 2.2.

Proses evaluasi keamanan informasi harus sesuai dengan panduan yang tertera pada Indeks KAMI. Panduan ini bisa dijadikan pedoman yang penting bagi instansi pemerintah maupun perusahaan untuk memastikan

keamanan informasi dilakukan secara terstruktur dan menyeluruh. Untuk pertanyaan atau panduan yang akan digunakan dalam melakukan evaluasi sebagai berikut:

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

Tahap awal responden harus menentukan terlebih dahulu jenis sistem elektronik dalam instansi tersebut. Tujuan dari proses ini untuk mengkategorikan sistem eletronik ke dalam tingkat tertentu. Tingkat kategori rendah, kategori tinggi, dan tingkat kategori strategis sehingga dapat dipetakan dengan ketergantungannya terhadap penggunaan sistem elektronik. Berikut pada Tabel 2.2 merupakan contoh tampilan Kategori Sistem Elektronik pada Indeks KAMI.

Tabel 2. 2 Contoh tampilan Kategori Sistem Elektronik

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	A
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

Setiap karakteristik instansi, perusahaan atau organisasi memiliki status penilaian yang dibedakan menjadi A, B, dan C yang masing-masing memiliki bobot yang berbeda. Status penilaian A memiliki bobot 5, B memiliki bobot 2, sedangkan C memiliki bobot 1. Dengan adanya status penilaian ini, tingkat ketergantungan terhadap sistem elektronik dapat diketahui.

Setiap area memiliki elemen penting untuk tercapainya tujuan keamanan masing-masing area. Untuk mencapai standar minimum Indeks KAMI, diperlukan pemenuhan SNI/IEC 27001:2013. Berikut adalah tampilan daftar pertanyaan untuk area II – VII beserta penjelasan komponennya.

Tabel 2. 3. Contoh Tampilan Area II - VII

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Fungsi/Organisasi Keamanan Informasi**		
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggung jawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Diterapkan Secara Meny	3
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggung jawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
2.3	II		Apakah pejabat/petugas pelaksana pe anan informasi mempunyai wewenang yang sesuai u enerapkan dan menjamin kepatuhan program keamana nformasi?	Diterapkan Secara Menyeluruh	3
2.4	II	1	Apakah penanggung jawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Diterapkan Secara Menyeluruh	3
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	3

Tabel 2.3 menunjukkan ilustrasi daftar pertanyaan area II – VII, di mana setiap daftar pertanyaan memiliki komponen yang sama dan

berikut ini keterangannya pada lingkaran merah yang sudah diberi angka:

1. Tingkat Kematangan
2. Kategori Pengamanan
3. Daftar Pertanyaan
4. Status Penerapan
5. Skor

Untuk setiap pemilihan jawaban yang tertera pada pertanyaan memiliki bobot yang berbeda. Berikut Tabel 2.4 yang merupakan hubungan antara status pengamanan, dan kategori pengamanan.

Tabel 2. 4 Matriks Bobot Status Penerapan dan Kategori Pengamanan

	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 di atas merupakan pemetaan bobot dan status yang ada di setiap area yang didapatkan. Berikut di bawah ini merupakan indikator kategori pengamanan.

Tabel 2. 5 Indikator Kategori Pengamanan

Kategori Pengamanan	Area Evaluasi				
	Tata Kelola	Risiko	Kerangka Kerja	Pengelola Aset	Teknologi
1	8	10	12	24	14
2	8	4	10	10	10
3	6	2	7	4	2
Maksimal Skor	126	72	159	168	120

Berdasarkan tabel 2.5 merupakan jumlah setiap kategori pengamanan dari 1-3 yang memiliki total skor keseluruhan yaitu 645. Berikut ini jumlah pertanyaan kematangan dan pengamanan:

Tabel 2. 6 Jumlah Pertanyaan Kematangan dan Pengamanan

Tingkat Kematangan	Kategori Pengamanan	Area Evaluasi				
		Tata Kelola	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 di atas menjabarkan jumlah pertanyaan yang dibagi di setiap area evaluasi berdasarkan tingkat kematangan dan kategori pengamanan. Pertanyaan tiap area akan digunakan sebagai alat untuk memberikan gambaran dan penilaian. Selanjutnya, dilakukan penentuan tingkat kesiapan area dalam penerapan SMKI yang dapat dilihat pada Tabel 2.7:

Tabel 2. 7 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

Berdasarkan Tabel 2.7 merupakan pengelompokan tingkat kematangan maka tingkat kematangan yang ada di Indeks KAMI dapat di definisikan sebagai berikut:

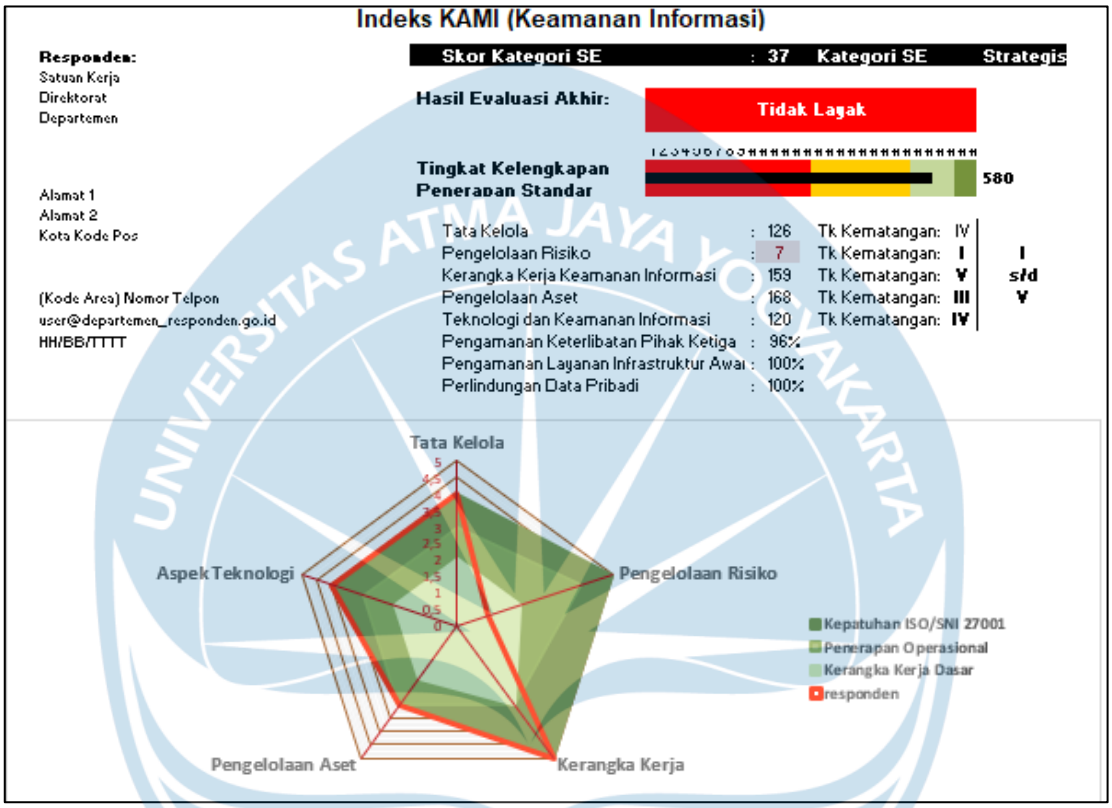
- Tingkat I – Kondisi Awal
- Tingkat II – Penerapan Kerangka Kerja Dasar
- Tingkat III – Terdefinisi dan Konsisten
- Tingkat IV – Terkelola dan Terukur
- Tingkat V - Optimal

Untuk memberikan uraian yang lebih detail tingkatan ini dapat ditambahkan "+" tergantung total skor menyentuh ambang batas tingkat kematangan, sehingga yang didapat ada 9 total tingkat kematangan yaitu I, I+, II, II+, III, III+, IV, IV+, dan V. untuk melihat rentang kelengkapan pengamanan yang digambarkan dapat dilihat pada gambar dibawah ini.

Gambar 2. 1 Rentang Tingkat Kematangan Indeks KAMI

Dilihat gambar diatas, level III+ merupakan minimum yang harus dicapai untuk dapat dikatakan layak menurut ISO/IEC 27001. jika hasil penilaian dibawah batas minimum standar ISO/IEC 27001 maka instansi,

perusahaan atau organisasi wajib meningkatkan kesiapan keamanan informasinya. *Dashboard* yang dimiliki indeks KAMI berisikan hasil nilai dari semua area yang sudah di evaluasi. Gambar 2.2 berikut ini, merupakan contoh *dashboard* penilaian keamanan informasi menggunakan Indeks KAMI.



Gambar 2. 2 Contoh Dasbor Penilaian Indeks KAMI