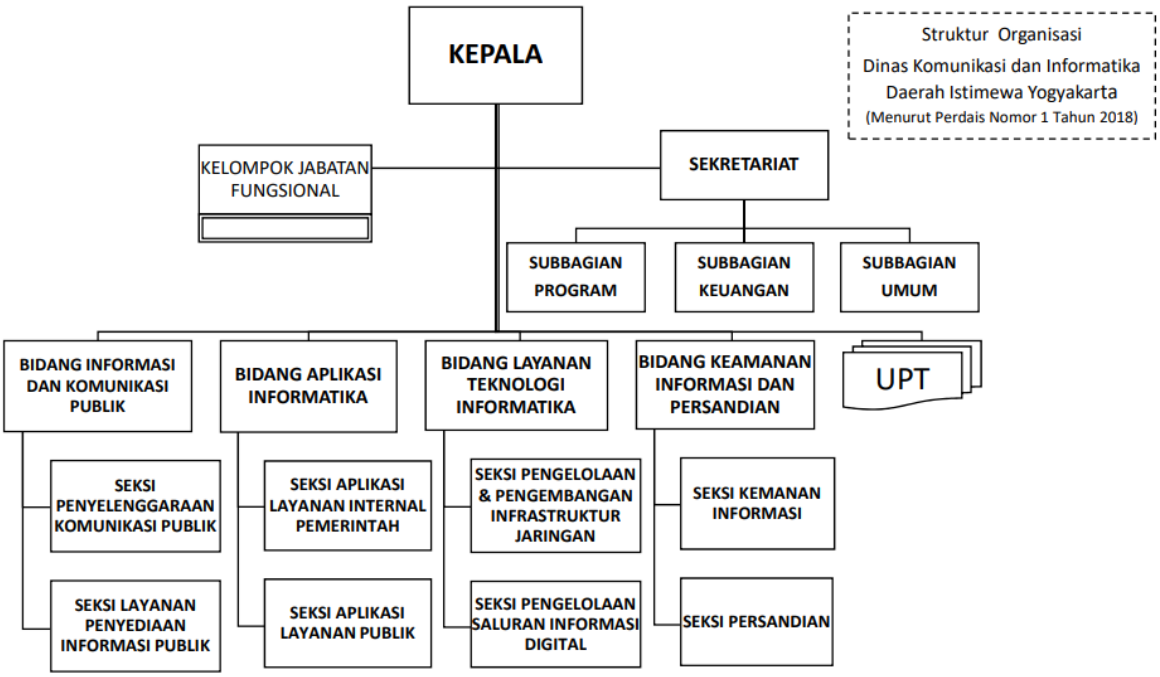
BAB 2
Tinjauan Pustaka

2.1 Objek Penelitian

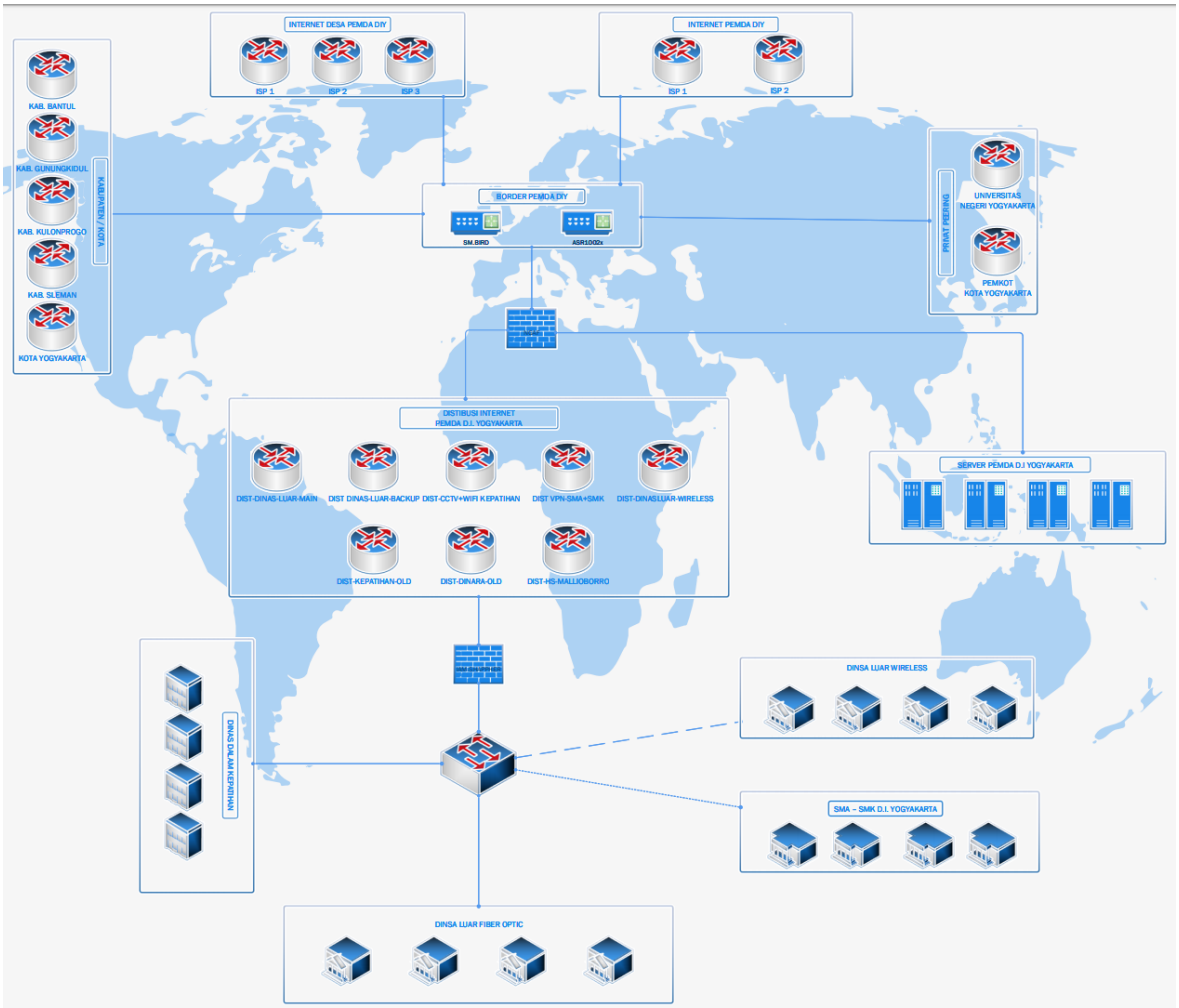
Bidang LTI adalah salah satu unit kerja dari Dinas Kominfo Pemda DIY yang bertugas melaksanakan pelayanan teknologi informatika Pemda DIY. Fungsi Bidang LTI diantaranya seperti pemangku kebijakan teknis terkait layanan teknologi informatika, pengelolaan dan pengembangan jaringan dan mengelola saluran informasi digital di lingkup Pemda DIY. Bidang LTI dalam struktural berada seperti Bidang lainnya di bawah Kepala Dinas, dan memiliki 2 seksi yaitu Seksi Pengelolaan dan Pengembangan Infrastruktur Jaringan; dan Seksi Pengelolaan Saluran Informasi Digital. Diskominfo Pemprov DIY (2019). Struktur Organisasi dari Dinas Kominfo DIY ditunjukkan dalam Gambar 2.1 di bawah.



Gambar 2.1 Struktur Organisasi Dinas Kominfo DIY tahun 2019

Bidang LTI sering mengalami masalah yang bersumber dari sisi pengguna namun berdampak hingga sisi pengelola. Terjadinya serangan di sisi pengguna menjadikan kinerja distribusi pada sisi pusat terganggu dan membuat jaringan pusat dan Organisasi Perangkat Daerah (OPD) atau Unit kerja lainnya (lihat Gambar 2.2) mengalami *down*. Kejadian seperti itu belum dapat diketahui secara pasti sebelum adanya laporan oleh pihak

pengguna. Sisi pengelola juga masih lemah akan kesadaran keamanan informasi, khususnya keamanan jaringan komputer sehingga kurangnya pantauan terhadap lalu lintas yang ada.



Gambar 2.2 Topologi Jaringan Pemda DIY

2.2 Penelitian Terkait

Penelitian tentang keamanan informasi dalam lingkup pemerintahan yang pernah dilakukan oleh Pratama, Suprapto, Perdanakusuma (2018) dilakukan di Dinas Kominfo Provinsi Jawa Timur (Kominfo Jatim). Dalam penelitian tersebut menjelaskan bahwasannya Kominfo Jatim semakin berkembang mengurusi informasi dan data yang dianggap penting. Oleh karenanya perlu dilakukan pengujian tingkat kematangan dan kesiapan terhadap keamanan informasi menggunakan pengukuran Indeks KAMI versi 3.1. Peneliti menambahkan acuan ISO 27001:2013 sebagai kontrol dari pengujian Indeks KAMI. Hasil yang didapatkan berupa nilai dari Indeks KAMI yang menunjukkan tingkat

kelengkapan dan kematangan keamanan informasi dari Kominfo Jatim masih rendah dan berada pada tingkat “tidak layak” dalam hasil Indeks KAMI. Peneliti kemudian menambahkan rekomendasi berupa kontrol ISO yang menerapkan beberapa klausul untuk membantu Kominfo Jatim sehingga dapat dinyatakan layak melakukan sertifikasi ISO27001 dan mengelola keamanan informasi pada instansi tersebut.

Penelitian berikutnya meneliti Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS. Basyarahil, Astuti, Hidayanto (2017) dalam penelitian tersebut mengevaluasi manajemen keamanan informasi dengan menggunakan Indeks KAMI dan ISO 27001:2013 sebagai kontrol. Masalah yang dialami oleh DPTSI ITS berdasarkan data yang diperoleh adalah banyak ditemukan celah keamanan pada jaringan komputer dan sistem informasi yang ada di kampus tersebut. Ditambah, beberapa kali terjadi serangan yang mengakibatkan gangguan terhadap kegiatan civitas akademika di ITS. Pengukuran dilakukan mengunakan Indeks KAMI versi 3.1 dan ISO27001:2013 sebagai kontrol terhadap hasil yang didapatkan. Dari penelitian tersebut, dapat disimpulkan bahwa DPTSI ITS belum siap dan belum matang untuk mengikuti sertifikasi ISO 27001:2013. Hal tersebut disebabkan karena kurangnya nilai yang didapat pada area pengelolaan resiko keamanan informasi karena belum diterapkan secara maksimal. Hasil yang minim pada area – area tersebut kemudian diberikan rekomendasi sesuai kontrol ISO 27001:2013 supaya kedepannya dapat diterapkan dan mendapatkan skor lebih baik.

Masih dalam ranah institusi pendidikan, terkait dengan Keamanan Informasi. Asriyanik, dan Prajoko (2018) melakukan penelitian tentang manajemen resiko keamanan informasi dengan menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI). Penelitian tersebut dirasa perlu dilakukan karena SIAK di UMMI sudah terintegrasi dengan jaringan dan dapat diakses secara daring melalui internet. Dengan pengembangan tersebut, dikhawatirkan terjadi serangan terhadap SIAK sehingga diharapkan dengan mempersiapkan manajemen resiko akan dapat mengurangi kemungkinan terjadinya serangan terhadap SIAK maupun meminimalkan dampak ketika terjadi serangan. Dalam penelitian tersebut menggunakan standar ISO 27005:2011 sebagai acuan proses manajemen resiko keamanan informasi, kemudian melakukan wawancara dan diskusi dari pengelola SIAK UMMI. Hasil yang didapatkan dari penilaian manajemen resiko keamanan informasi dengan kontrol ISO 27001:2011, pengelola harus dapat mempersiapkan terhadap 47 dari 73 skenario serangan karena belum bisa diselesaikan oleh pengendalian yang ada. Pemilihan pengendalian

resiko juga terbagi menjadi 19 poin diharuskan melakukan modifikasi, 1 resiko ditransfer, dan 27 resiko dihindari.

Penelitian berikutnya berupa parade paper yang membahas tentang aspek keamanan sistem informasi dilihat dari sisi aspek kemanusiaan yang dilakukan oleh Shouran, Priyambodo, Ashari (2019). Dalam penelitian tersebut menjelaskan bahwa keamanan sistem informasi dipengaruhi oleh beberapa aspek, seperti aspek data itu sendiri, aspek kebijakan, aspek infrastruktur, aspek teknologi, dan aspek manusia. Dijabarkan juga aspek manusia arahnya adalah kurangnya kesadaran dan perilaku berbahaya dalam menggunakan sistem informasi itu sendiri, termasuk di dalamnya membuat, menggunakan, hingga menghapus. Diskusi yang diberikan dalam penelitian tersebut mengarahkan penggunaan standart untuk keamanan sistem informasi, seperti ISO untuk mengenalkan kesadaran dalam keamanan sistem informasi. Sebagai penutup, peneliti menyimpulkan bahwa kesadaran keamanan informasi merupakan cara untuk mengurangi ancaman serangan yang mengarah ke kelemahan manusia itu sendiri.

Selanjutnya terdapat penelitian studi pustaka tentang konsep dan strategi evaluasi manajemen keamanan informasi menggunakan indeks KAMI dan evaluasi kesadaran keamanan informasi pada pengguna. Penelitian tersebut dilakukan oleh Budi, Tarigan (2018) guna merumuskan konsep strategi evaluasi manajemen keamanan informasi dan kesadaran keamanan informasi pada pengguna, berikut konsep yang mendukungnya. Dalam penelitian tersebut dijelaskan area dari Indeks Kami dan konsep evaluasi kesadaran keamanan informasi pada pengguna menggunakan metode evaluasi *Human Aspects of Information Security Questionnaire* (HAIS-Q). Hasil yang didapatkan adalah sebuah tahapan – tahapan dalam melaksanakan evaluasi Indeks KAMI dan berbarengan dengan evaluasi HAIS-Q untuk menilai tingkat kesadaran keamanan pada pengguna.

Penelitian berikutnya adalah tentang pengukuran kesadaran keamanan informasi menggunakan metode *Multiple Criteria Decision Analysis* (MCDA) yang mengambil studi kasus pada pengguna perangkat maupun aplikasi yang menyangkut keamanan informasi di kantor pemerintahan. Penelitian yang dilakukan oleh Kusumawati (2018) banyak mengambil bahan dari sikap, perilaku, dan pengetahuan akan kesadaran keamanan informasi. Permodelan tersebut berasal dari penelitian terdahulu yang dilakukan oleh Kruger dan Kearney di tahun 2005 silam. Dari permodelan tersebut, peneliti mendapatkan area – area yang dapat dijadikan menjadi objek penelitian dan dapat dikembangkan menjadi pertanyaan di kuisioner. Hasil yang didapatkan kemudian dikalkulasi menggunakan MCDA supaya mendapatkan prosentase dari nilai kesadaran keamanan

informasi di kantor pemerintahan tersebut. Hasil yang didapatkan yakni pengguna masih berada pada level menengah dan dengan acuan tersebut maka diharapkan dapat meningkatkan tingkat kesadaran keamanan informasi terutama pada area pengetahuan tentang *best practice* keamanan informasi.

Penelitian terakhir yang dijadikan acuan datang dari studi literatur milik Babtain, Halabi, Karrar (2019) yang membahas tentang kebijakan keamanan informasi yang berada pada suatu sistem atau organisasi. Kebijakan tersebut banyak digunakan sebagai asuransi terhadap data – data yang digunakan oleh pengguna. Kepercayaan pengguna sebagai objek penelitian dijadikan patokan dalam peneliti menilai dari setiap kebijakan yang ada. Seperti dalam penyusunan kebijakan, banyak dipengaruhi oleh aspek – aspek yang mengedepankan kepercayaan dari pengguna itu sendiri.

Penelitian lain dilakukan oleh Arfanudin, Sugiantoro, Prayudi(2017) dilakukan di Dinas Kominfo Kota Tegal memuat tentang *monitoring traffic* serangan pada router dinas tersebut menggunakan *security information event and management* (SIEM) dan implikasinya terhadap nilai Indeks KAMI. Dalam penelitian tersebut dijelaskan mengenai penilaian Indeks KAMI sebelum diberlakukan pemantauan teradap *router* pusat milik Dinas tersebut dan kemudian dilakuan percobaan uji coba serangan dan dilakukan penilaian ulang. Hasil yang didapatkan adalah ketika menggunakan SIEM, 4 dari 8 aktivitas serangan yang dilakukan dapat dipantau serta dapat menaikkan skor pada salah satu area Indeks KAMI.

Penelitian yang diusulkan oleh peneliti yaitu meneliti kesadaran keamanan/*security awareness* dilakukan pada Bidang LTI Kominfo DIY, menggunakan Indeks KAMI sebagai *scoring*, dan memanfaatan *report* dari NGFW sebagai acuan. Ringkasan dari pembahasan penelitian terkait tersebut terdapat pada Tabel 2.1 di bawah ini.

Tabel 2.1 *Literature Review*

No	Peneliti	Uraian	Objek Penelitian	Hasil
1	Edo Rizky Pratama, Suprapto, Andi Reza Perdanakusuma (2018)	Penelitian tentang evaluasi kelayakan Dinas Kominfo Jatim dalam rangka menuju sertifikasi ISO27001	Evaluasi SKTI menggunakan Indeks KAMI dan kontrol ISO27001	Hasil dari nilai Indeks KAMI akan dijadikan rekomendasi dengan acuan klausul ISO 27001 sebagai kontrol terhadap aktivitas yang ada.

		menggunakan Indeks KAMI.		
2	Basyarahil, Astuti, Hidayanto (2017)	DPTSI ITS Surabaya menyatakan ada celah keamanan informasi dan jaringan yang dinilai cukup berbahaya. Peneliti melakukan evaluasi terhadap manajemen keamanan informasi dengan menggunakan Indeks KAMI	Evaluasi Manajemen Keamanan Informasi pada DPTSI ITS Surabaya menggunakan Indeks KAMI	Penelitian tersebut membahas tentang kesiapan DPTSI ITS Surabaya dalam menuju ISO27001, dengan tetap memberikan rekomendasi untuk dapat memperbaiki nilai dari Indeks KAMI.
3	Asriyanik, dan Prajoko (2018)	Universitas Muhammadiyah Sukabumi (UMMI) berencana untuk menggunakan SIAK secara daring, maka diperlukan penyusunan dan evaluasi manajemen resiko yang dapat membantu mengamankan SIAK tersebut.	Evaluasi Manajemen Resiko Keamanan informasi menggunakan ISO 27005:2013 terhadap SIAK UMMI	Manajemen Resiko Keamanan Informasi ISO 27005:2013 termasuk dalam sub standardisasi ISO 27001:2013, sehingga manajemen resiko keamanan informasi dinilai sudah cukup untuk mengurangi ancaman serangan terhadap SIAK UMMI.
4	Shouran, Priyambodo, Ashari (2019)	Dalam penelitian tersebut menjelaskan bahwa keamanan sistem informasi dipengaruhi salah	Aspek – aspek yang mempengaruhi dalam keamanan informasi, dan	Mengetahui keterkaitan aspek keamanan sistem informasi dengan aspek kemanusiaan.

		satunya oleh aspek manusia. Dibanding dengan aspek – aspek lainnya, aspek tersebut dinilai lebih krusial karena penggunaan yang salah dapat membawa kepada kerentanan keamanan informasi.	bagaimana perusahaan dapat meminimalisir kerentanan tersebut dengan standardisasi ISO 27001	
5	Budi, Tarigan (2018)	Studi pustaka mengenai langkah – langkah dalam evaluasi manajemen keamanan informasi.	Evaluasi Manajemen keamanan informasi dengan Indeks KAMI dan HAIS-Q	merumuskan konsep strategi evaluasi manajemen keamanan informasi dan kesadaran keamanan informasi pada pengguna, berikut konsep yang mendukungnya.
6	Kusumawati (2018)	Penelitian dilakukan dengan harapan bagaimana sebuah organisasi dapat meningkatkan sikap dan perilaku anggotanya supaya awas dan sadar akan keamanan informasi.	Perilaku dan sikap dari karyawan dalam suatu organisasi menggunakan metode *Multiple Criteria Decission Analysis*(MCDA)	Menghitung kesadaran keamanan informasi menggunakan metode MCDA.
7	Babtain, Halabi, Karrar (2019)	Penelitian dilakukan secara studi literatur terhadap ranah *information security policies' compliance* (ISPC). Bagaimana	Studi literatur terhadap berbagai makalah yang membahas ISPC.	Penyusunan kebijakan terkait keamanan informasi perlu memperhatikan berbagai macam aspek guna memupuk kepercayaan terhadap

		memaksimalkan kebijakan untuk meningkatkan kepercayaan pengguna terhadap keamanan informasi.		pengguna.
8	Arfanudin , Sugiantoro, Prayudi (2017)	Penelitian mengambil data pada Dinas Kominfo Kota Tegal. Menggunakan software SIEM untuk memantau skenario serangan pada *traffic* router yang ada.	Skenario serangan pada *traffic* router Dinas Kominfo Kota Tegal	Hasil yang didapatkan adalah menggunakan SIEM, 4 dari 8 aktivitas serangan yang dilakukan dapat dipantau serta dapat menaikkan skor pada area teknologi dan keamanan informasi.
9	Penelitian yang diusulkan	Penelitian terhadap kesadaran keamanan dilakukan pada Bidang LTI Kominfo DIY, menggunakan Indeks KAMI sebagai *scoring* dengan memanfaatkan *report* dari NGFW sebagai acuan.	Kesadaran keamanan informasi pada Bidang LTI Kominfo DIY menggunakan Indeks KAMI	Menggunakan *report* NGFW sebagai bahan acuan untuk pihak individu Bidang LTI meningkatkan kesadaran keamanan informasi pada Bidang kerjanya.

2.3 Dasar Teori

2.3.1 NGFW

Firewall tradisional menyediakan inspeksi pada *traffic* jaringan dengan melakukan *filter* paket yang lewat dari port, protokol, sesuai dengan yang didefinisikan oleh administrator jaringan tersebut. Sedangkan *Next Generation Firewall* (NGFW) memiliki akses lebih luas dan lebih dalam. NGFW dapat melakukan inspeksi paket lebih dalam hingga level aplikasi.

Penggunaan NGFW dapat membantu pengamanan jaringan yang lebih baik lagi. Luntovskyy, Klimash (2017)

2.3.2 Sangfor NGAF

Sangfor NGAF adalah salah satu produk untuk solusi NGFW yang memberikan proteksi terhadap serangan hingga *endpoint*, seperti *malware*, virus, *ransomware*, hingga serangan web. Dalam Sangfor NGAF terdapat *firewall* secara umum, *web application firewall*(WAF), *threat prevention, data leakage prevention, user access management, ips, visibility report,* dan *risk assessment*. Selain itu juga terdapat *antivirus, antimalware* untuk proteksi pada sisi *endpoint* / pengguna. Sangfor (2019)

2.3.3 Indeks KAMI

Indeks KAMI (Keamanan Informasi) merupakan alat terbitan dari Badan Siber dan Sandi Negara (BSSN) yang digunakan untuk membantu menganalisa dan mengevaluasi tingkat kesiapan penerapan keamanan informasi di suatu organisasi. Indeks KAMI menggunakan SNI ISO/IEC 27001:2013 sebagai acuan utama dan dibagi menjadi 5 aspek yang terdiri dari:

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

Indeks KAMI terbaru adalah versi 4.0, yang diluncurkan pada Maret 2019 oleh BSSN, dan dapat diunduh pada website bssn.go.id/indeks-kami/. Indeks KAMI versi 4.0 memiliki update penambahan area suplemen yang berisi manajemen pengamanan terhadap keterlibatan pihak ketiga, pengamanan infrastruktur *cloud*, dan pengamanan terhadap data pribadi. Suplemen tersebut tidak mempengaruhi nilai utama dalam skor 5 area sebelumnya. Indeks KAMI dianjurkan untuk dapat diisi oleh pejabat berwenang dalam mengelola keamanan informasi di cakupan instansinya. BSSN (2019)

Indeks KAMI memiliki 2 keperluan dalam penilaiannya, yang pertama adalah tingkat kesiapan sesuai dengan kelengkapan kontrol SNI ISO/IEC27001:2013 yang dibagi menjadi 3 kategori (lihat Gambar 2.3). Kategori 1 adalah kerangka kerja dasar keamanan, Kategori 2 berupa efektifitas dan konsistensi, dan kategori 3 adalah kemampuan untuk meningkatkan kinerja. Dari penilaian tersebut lalu akan dijumlahkan dan didapati skor total

yang kemudian akan dibandingkan dengan hasil dari Kategori sistem elektronik sehingga didapatkan nilai akhir dari 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 Penilaian dalam status berdasarkan kategori pengamanan

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 2.4 Kategori Sistem Elektronik

Berdasarkan skor tiap area dan kategori, kemudian dapat dihitung nilai kematangan penerapan pengamanan dengan dibagi berdasarkan penilaian kerangka kerja COBIT atau CMMI. Tingkatan tersebut dibagi menjadi 9 tingkatan sebagai berikut:

1. Tingkat I – Kondisi Awal
2. Tingkat II – Penerapan Kerangka Kerja Dasar
3. Tingkat III – Terdefinisi dan Konsisten
4. Tingkat IV – Terkelola dan Terukur
5. Tingkat V – Optimal

4 tingkatan selain yang disebutkan di atas adalah I+, II+, III+ dan IV+ sebagai uraian tingkatan yang lebih detail. Tingkat kematangan yang diharapkan untuk ambang batas minimum adalah Tingkat III+. BSSN (2019)

2.3.4 Security Awareness

Security awareness adalah kondisi manusia sadar akan keamanan, dalam hal ini merupakan keamanan informasi atau keamanan sistem infomasi. *Security aware* erat kaitannya dengan manajemen risiko karena dapat meminimalisir risiko yang berkaitan dengan keamanan informasi atau keamanan system informasi. Tantangan dalam Organisasi yang bergerak di bidang Teknologi Informasi adalah menanamkan kesadaran keamanan terhadap anggotanya, hal ini didasarkan oleh sisi manusia dapat menjadi titik lemah yang cukup fatal dalam menjaga keamanan informasi tersebut. Shouran, Priyambodo, Ashari(2019)