BADAN SIBER DAN SANDI NEGARA

LAPORAN
Penilaian Mandiri

Indeks Keamanan Informasi (KAMI)
Kabupaten Pesisir Selatan
Tahun 2024

Dinas Komunikasi dan Informatika
Pemerintah Kabupaten Pesisir Selatan

Jl. Dr. M. Hatta – Painan , (0756) 231 2227
Email : diskominfo@mail.pesisirselatankab.go.id
Email CSIRT : csirt@mail.pesisirselatankab.go.id

KATA PENGANTAR

Dengan menghaturkan puji dan Syukur kehadirat Allah SWT karena berkat petunjuk dan hidayah-Nya, Laporan Tingkat Keamanan Informasi Pemerintah melalui Indeks KAMI (Keamanan Informasi) yang masih Peniliaian Mandiri atau *self assessment*, dapat diselesaikan sesuai dengan jadwal yang direncanakan.

Laporan Indeks KAMI ini merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001, yang mengacu pada tugas pokok dan fungsi yang diemban.

Sebagai salah satu unsur dari fungsi Persandian, Dinas Komunikasi dan Informatika khususnya pada Seksi Persandian Bidang Statistik dan Persandian telah menjalankan serangkaian kegiatan, yang berfokus pada evaluasi tingkat keamanan Indeks KAMI dengan menggunakan versi 5.0 sebagai padanan terhadap standar ISO/IEC 2700: 2013.

Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada Pimpinan Instansi. Implementasi Indeks KAMI dilakukan oleh penyelenggara layanan publik secara elektronik melalui Bimbingan Teknis, Asesmen, dan Konsultasi.

Painan, Desember 2024

Indeks KAMI (Keamanan Informasi) Versi 5.0

Responden:
Dinas Komunikasi dan Informatika
Pemerintah Kabupaten Pesisir Selatan

Jl. Dr. Moh Hatta, Painan. 25611
Kecamatan IV Jurai.
Kabupaten Pesisir Selatan

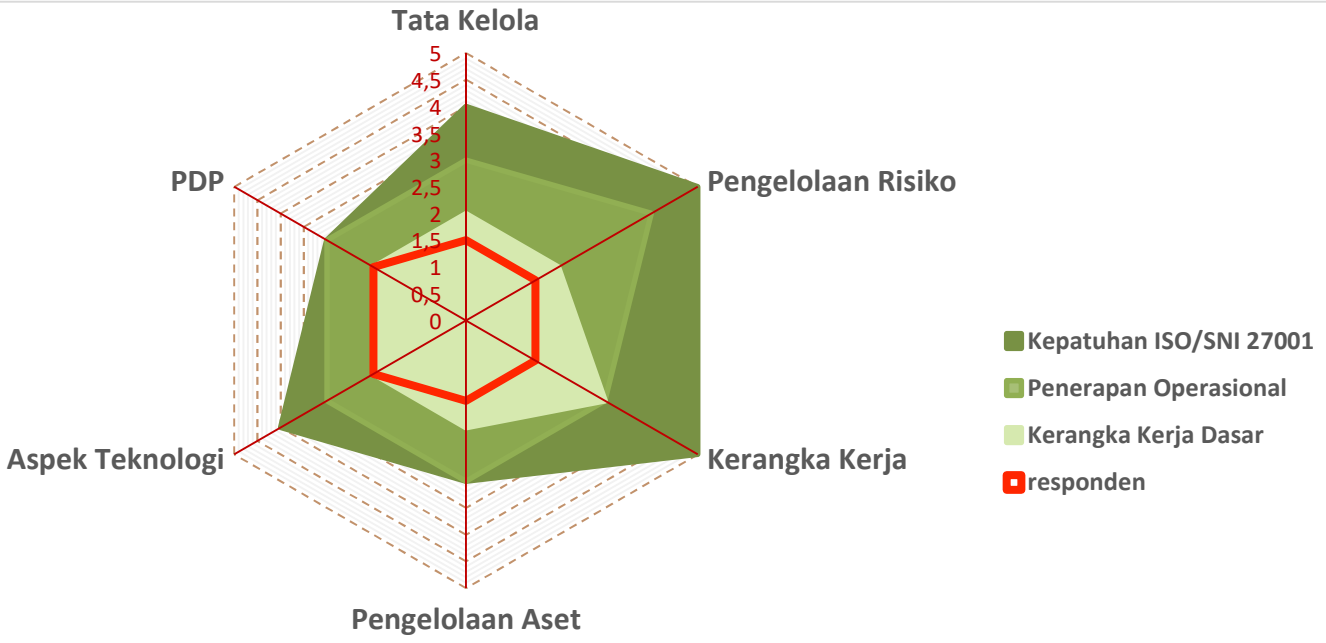
(0756) 231 22271
diskominfo@mail.pesisirselatankab.go.id
21/11/2024

Skor Kategori SE	:	23	Kategori SE	Tinggi

Hasil Evaluasi Akhir: **Pemenuhan Kerangka Kerja Dasar**

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori — 388

Tata Kelola	:	48	T. Kematangan:	I+	
Pengelolaan Risiko	:	22	T. Kematangan:	I+	I+
Kerangka Kerja Keamanan Informasi	:	53	T. Kematangan:	I+	s/d
Pengelolaan Aset	:	120	T. Kematangan:	I+	II
Teknologi dan Keamanan Informasi	:	113	T. Kematangan:	II	
Pelindungan Data Pribadi	:	32	T. Kematangan:	II	
Pengamanan Keterlibatan P.Ketiga	:	7	%		



Indeks Keamanan Informasi (Indeks KAMI)

Identitas Instansi atau Perusahaan	*Dinas Komunikasi dan Informatika* *Pemerintah Kabupaten Pesisir Selatan*
Alamat	*Jl. Dr. Moh Hatta, Painan. 25611* *Kecamatan IV Jurai.* *Kabupaten Pesisir Selatan*
Nomor Telpon	*(0756) 231 22271*
Email	diskominfo@mail.pesisirselatankab.go.id
Pengisi Lembar Evaluasi	*Muhammad Azmi Riyan, S.Kom*
Jabatan	*Sandiman Ahli Pertama*
Tanggal Pengisian	*21/11/2024*

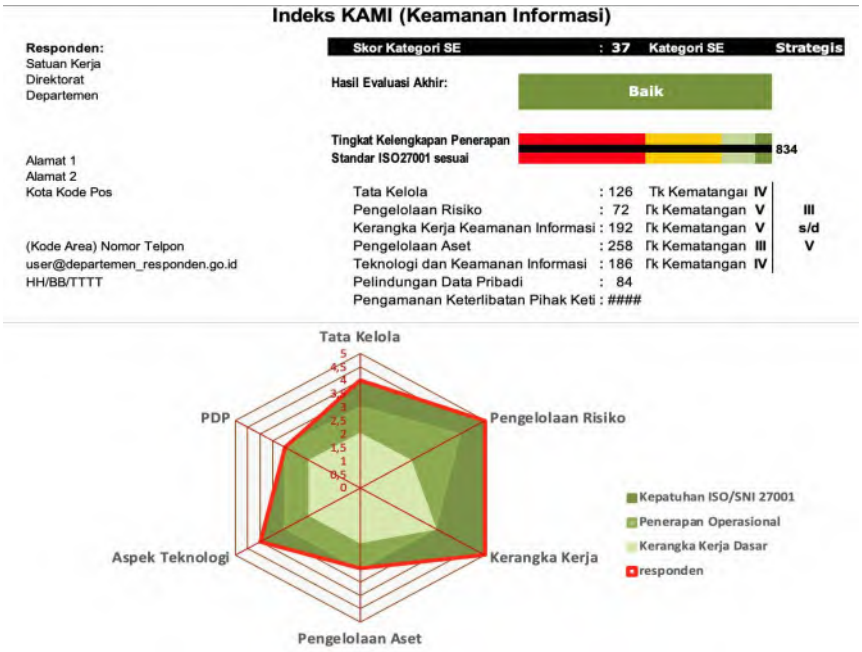
Deskripsi Ruang Lingkup

Isi dengan deskripsi ruang lingkup struktur organisasi (Departemen, Bagian atau Satuan Kerja) dan infrastruktur TIK

Indeks Keamanan Informasi (Indeks KAMI)

Versi 5.0, Maret 2023

Mengenai Indeks KAMI



Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2022.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya proses yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan *snapshot* indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (*stakeholders*).

Khusus untuk Instansi Pemerintah, penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi. Pertukaran informasi dan diskusi dengan Instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari lesson learned yang sudah dilalui.

Petunjuk Penggunaan Alat Evaluasi Indeks Keamanan Informasi (Indeks KAMI)

Alat evaluasi Indeks KAMI ini dapat digunakan oleh organisasi dengan skala nasional, maupun yang berukuran kecil. Penggunaan di Instansi pemerintah dapat dilakukan di tingkat pusat maupun satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggungjawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya.

Proses evaluasi dilakukan melalui sejumlah pertanyaan di masing-masing area di bawah ini:
- Kategori Sistem Elektronik yang digunakan Instansi
- Tata Kelola Keamanan Informasi
- Pengelolaan Risiko Keamanan Informasi
- Kerangka Kerja Keamanan Informasi
- Pengelolaan Aset Informasi, dan
- Teknologi dan Keamanan Informasi
- Pelindungan Data Pribadi
- Suplemen: Area evaluasi untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan.

Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan kondisi penerapan keamanan informasi SESUNGGUHNYA. Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan azas keterbukaan dan kejujuran.

Sebelum mulai menjawab pertanyaan terkait kesiapan pengamanan informasi, responden diminta untuk mendefinisikan Kategori Sistem Elektronik di Instansinya. Definisi ini bisa dijabarkan untuk tingkat Satuan Kerja baik di tingkat Kementerian/Lembaga, ataupun untuk satuan kerja yang lebih kecil, sampai ke Unit Eselon III. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan Sistem Elektronik yang digunakan instansi ke "tingkat" tertentu: Rendah, Tinggi dan Strategis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik Sistem Elektornik yang sama.

Pertanyaan dikelompokkan untuk 2 keperluan. Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan **kelengkapan** kontrol yang diminta oleh standar ISO/IEC 27001:2022. Dalam pengelompokan ini responden diminta untuk memberi tanggapan mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (pertanyaan diberi label "1"), efektifitas dan konsistensi penerapannya (label "2"), sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (label "3"). Tingkat terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar ISO/IEC 27001:2022.

Setiap jawaban diberikan skor yang nantinya dikonsolidasi untuk menghasilkan angka

	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

(Catatan: untuk keseluruhan area pengamanan, pengisian pertanyaan dengan label "3" hanya dapat memberikan hasil/nilai apabila semua pertanyaan dengan label "1" sudah diisi dengan status "Diterapkan Menyeluruh" dan/atau paling rendah hanya terdapat status "Diterapkan Sebagian" maksimal sebanyak dua).

Hasil dari penjumlahan skor untuk masing-masing area ditampilkan dalam diagram radar dengan latar belakang area untuk tingkat maksimal kematangan 1 s/d 3. Dalam diagram ini bisa dilihat perbandingan antara kondisi kesiapan sebagai hasil dari proses evaluasi dengan acuan tingkat kematangan yang ada.

Dengan membaca diagram ini, pimpinan instansi dapat melihat kebutuhan pembenahan yang diperlukan dan korelasi antara berbagai area penerapan keamanan informasi. Adapun korelasi antara Kategori Sistem Elektronik dengan Status Kesiapan didefinisikan melalui tabel berikut:

KATEGORI SISTEM ELEKTRONIK				
Rendah		**Skor Akhir**		**Status Kesiapan**
10	15	0	247	Tidak Layak
		248	443	Pemenuhan Kerangka Kerja Dasar
		444	760	Cukup Baik
		761	916	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	387	Tidak Layak
		388	646	Pemenuhan Kerangka Kerja Dasar
		647	828	Cukup Baik
		829	916	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	472	Tidak Layak
		473	760	Pemenuhan Kerangka Kerja Dasar
		761	864	Cukup Baik
		865	916	Baik

Pengelompokan kedua dilakukan berdasarkan tingkat **kematangan** penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh keangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga.

Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai:

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

Untuk membantu memberikan uraian yang lebih detil, tingkatan ini ditambah dengan tingkatan antara - I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan Tingkat I. Sebagai padanan terhadap standar ISO/IEC 2700:2013, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.

Ilustrasi di bawah menunjukkan label pengelompokan kematangan (kolom di sebelah kanan nomor urut) dan kelengkapan (kolom di sebelah kiri pertanyaan).

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

Kedua pengelompokan ini dapat dipetakan (lihat gambar di bawah) untuk memberikan dua sudut pandang yang berbeda: tingkat kelengkapan pengamanan dan tingkat kematangan pengamanan. Instansi responden dapat menggunakan metrik ini sebagai target program keamanan informasi.

Indeks KAMI sebaiknya digunakan 2X dalam setahun sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu.

Suplemen

Perkembangan teknologi yang pesat dan pola bisnis yang dinamis menyebabkan munculnya risiko keamanan informasi baru. Keterlibatan pihak ketiga dalam rantai pasok (supply chain) layanan suatu instansi/perusahaan menimbulkan risiko terkait keberadaan/keterlibatan pihak eksternal tersebut.

Untuk menilai kesiapan instansi/perusahaan dalam mengelola risiko di area baru ini, pada revisi 5.0 disediakan modul suplemen yang membahas aspek kesiapan pengamanan untuk ketiga aspek tersebut.
Penggunaan modul suplemen untuk evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga digunakan sesuai konteks atau cakupan yang ada. Responden hanya perlu menjawab area evaluasi yang berlaku.

Butir-butir evaluasi kesiapan pengamanan yang disusun untuk setiap area merupakan persyaratan dasar yang bagi instansi/perusahaan yang terpapar risiko terkait area tersebut.

Hasil penilaian evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga disampaikan dalam bentuk persentase (%) dengan obyektif/sasaran pencapaian maksimal.

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
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	B
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	A
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	B
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	A
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	C
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	B

Bagian I: Kategori Sistem Elektronik		
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan		
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**
1.9	Dampak dari kegagalan Sistem Elektronik [A] Membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik berskala nasional atau berdampak pada layanan di sektor lain [C] Tidak tersedianya layanan publik dalam 1 propinsi atau internal 1 instansi/perusahaan	C
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	C
	Skor penetapan Kategori Sistem Elektronik	**23**

Bagian II: Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi instansi/perusahaan beserta fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Fungsi/Organisasi Keamanan Informasi**	
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Penerapan / Diterapkan Sebagian
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Dalam Penerapan / Diterapkan Sebagian
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Penerapan / Diterapkan Sebagian
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Penerapan / Diterapkan Sebagian
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Dalam Penerapan / Diterapkan Sebagian
2.11	II	2	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Dalam Penerapan / Diterapkan Sebagian
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Dalam Perencanaan
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Diterapkan Secara Menyeluruh
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	Dalam Penerapan / Diterapkan Sebagian
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Dalam Penerapan / Diterapkan Sebagian
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Dalam Penerapan / Diterapkan Sebagian
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Dalam Perencanaan
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Penerapan / Diterapkan Sebagian
2.20	IV	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian
2.21	IV	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Penerapan / Diterapkan Sebagian
			Total Nilai Evaluasi Tata Kelola	**48**

Bagian III: Pengelolaan Risiko Keamanan Informasi

Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Kajian Risiko Keamanan Informasi**	
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Dalam Perencanaan
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	Dalam Perencanaan
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Perencanaan
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Penerapan / Diterapkan Sebagian
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Penerapan / Diterapkan Sebagian
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Penerapan / Diterapkan Sebagian
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Dalam Perencanaan
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Penerapan / Diterapkan Sebagian
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Dalam Perencanaan
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Dalam Perencanaan
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Dalam Perencanaan
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Dalam Perencanaan
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Dalam Perencanaan
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Dalam Penerapan / Diterapkan Sebagian
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	**22**

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

			[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	**Status**
#			**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**	
4.1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Perencanaan
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Dalam Perencanaan
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Dalam Perencanaan
4.4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?	Dalam Perencanaan
4.6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Dalam Perencanaan
4.7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Dalam Penerapan / Diterapkan Sebagian
4.9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?	Dalam Penerapan / Diterapkan Sebagian
4.10	III	2	Apakah instansi/perusahaan anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch,* alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Dalam Penerapan / Diterapkan Sebagian
4.11	III	2	Apakah instansi/perusahaan anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Dalam Penerapan / Diterapkan Sebagian
4.12	III	2	Apakah instansi/perusahaan anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Penerapan / Diterapkan Sebagian
4.13	III	2	Apakah instansi/perusahaan anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Dalam Penerapan / Diterapkan Sebagian
4.14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Dalam Penerapan / Diterapkan Sebagian
4.15	III	2	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab terkait perkembangan ancaman keamanan informasi dan pengelolaannya (*threat inteligence*)?	Dalam Perencanaan
4.16	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	Dalam Perencanaan
4.17	III	3	Apakah kebijakan dan prosedur yang diperlukan terkait perkembangan ancaman keamanan informasi dan pengelolaannya (*threat inteligence*) sudah disusun dan dituliskan dengan jelas (proses pengumpulan data, analisa, dan identifikasi ancaman), dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Perencanaan
4.18	III	3	Apakah hasil analisis perkembangan ancaman keamanan informasi disampaikan kepada pihak yang bertanggung jawab untuk mitigasi risiko, dan memantau perkembangan mitigasi tersebut?	Dalam Perencanaan
4.19	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Dalam Perencanaan
	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah menentukan Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) ? RTO - Tujuan yang ditetapkan instansi/perusahaan untuk jangka waktu maksimum yang diperlukan untuk memulihkan operasi normal setelah terjadi gangguan yang mengakibatkan berhentinya sistem RPO - Jumlah maksimum data yang dapat ditoleransi oleh instansi/perusahaan jika hilang. Parameter ini diukur dalam waktu: dari saat kegagalan terjadi hingga pencadangan data valid terakhir Anda.	Dalam Perencanaan
4.20	III	3	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan minimal sekali dalam setahun atau apabila ada keperluan yang mendesak (seperti perubahan infrastruktur), dilaksanakan sesuai jadwal penerapan perubahannya?	Dalam Perencanaan

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

			[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	**Status**
4.21	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Dalam Perencanaan
4.22	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Dalam Penerapan / Diterapkan Sebagian
#			**Pengelolaan Strategi dan Program Keamanan Informasi**	
4.23	II	1	Apakah instansi/perusahaan anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Dalam Penerapan / Diterapkan Sebagian
4.24	II	1	Apakah instansi/perusahaan anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Dalam Penerapan / Diterapkan Sebagian
4.25	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Dalam Penerapan / Diterapkan Sebagian
4.26	III	1	Apakah instansi/perusahaan anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Dalam Perencanaan
4.27	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Dalam Perencanaan
4.28	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Dalam Perencanaan
4.29	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Dalam Perencanaan
4.30	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Tidak Dilakukan
4.31	V	3	Apakah instansi/perusahaan anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Tidak Dilakukan
4.32	V	3	Apakah instansi/perusahaan anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Tidak Dilakukan
			Total Nilai Evaluasi Kerangka Kerja	**53**

Bagian V: Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pengelolaan Aset Informasi**	
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)	Dalam Penerapan / Diterapkan Sebagian
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Dalam Penerapan / Diterapkan Sebagian
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	Dalam Penerapan / Diterapkan Sebagian
5.5	II	1	Apakah tersedia proses untuk mengidentifikasi dan menginventarisir syarat retensi asset informasi sesuai dengan peraturan perundangan yang ada dan menghapusnya jika sudah melewati batas retensi tersebut	Dalam Penerapan / Diterapkan Sebagian
5.6	II	1	Apakah tersedia proses untuk mengevaluasi kepatuhan terhadap syarat retensi dan menghapus aset informasi jika sudah melewati batas retensi tersebut	Dalam Penerapan / Diterapkan Sebagian
5.7	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian
5.8	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian
5.9	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Dalam Penerapan / Diterapkan Sebagian
			Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
5.10	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Dalam Penerapan / Diterapkan Sebagian
5.11	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Dalam Perencanaan
5.12	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Dalam Perencanaan
5.13	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Diterapkan Secara Menyeluruh
5.14	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Dalam Penerapan / Diterapkan Sebagian
5.15	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Diterapkan Secara Menyeluruh
5.16	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Diterapkan Secara Menyeluruh
5.17	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dalam Penerapan / Diterapkan Sebagian
5.18	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Penerapan / Diterapkan Sebagian
5.19	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan / Diterapkan Sebagian
5.20	II	1	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	Dalam Penerapan / Diterapkan Sebagian
5.21	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Perencanaan
5.22	III	2	Proses pengecekan latar belakang SDM	Diterapkan Secara Menyeluruh
5.23	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Dalam Penerapan / Diterapkan Sebagian
5.24	III	2	Proses dan metoda untuk penghancuran informasi yang sudah tidak diperlukan dan sesuai dengan klasifikasi informasi (mis: secure delete, jenis/kerapatan shredder dll),Termasuk didalamnya laporan bukti penghancuran informasi ?	Dalam Perencanaan
5.25	III	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Dalam Perencanaan
5.26	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Dalam Penerapan / Diterapkan Sebagian
5.27	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Tidak Dilakukan
5.28	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak Dilakukan
5.29	III	3	Apakah telah diterapkan proses dan metoda untuk mengaburkan data (data masking) agar hanya dapat dilihat oleh pihak yang mempunyai otoritas sesuai regulasi atau kebijakan? Mis: pengamanan data pribadi, data sensitif	Dalam Penerapan / Diterapkan Sebagian
5.30	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/*vendor*) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Tidak Dilakukan

Bagian V: Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

			[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	**Status**
#			**Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)**	
5.31	III	2	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	Dalam Penerapan / Diterapkan Sebagian
5.32	III	2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?	Dalam Penerapan / Diterapkan Sebagian
5.33	III	2	Apakah instansi/perusahaan sudah menetapkan kebijakan dan menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?	Dalam Perencanaan
5.34	III	2	Apakah instansi/perusahaan sudah mengkaji, menetapkan pembagian tanggung jawab keamanan informasi antara perusahaan dan penyelenggara layanan cloud ?	Dalam Penerapan / Diterapkan Sebagian
5.35	III	2	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?	Dalam Penerapan / Diterapkan Sebagian
5.36	III	2	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?	Dalam Penerapan / Diterapkan Sebagian
5.37	III	2	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud,* termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	Dalam Perencanaan
5.38	III	2	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	Dalam Penerapan / Diterapkan Sebagian
5.39	III	2	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?	Dalam Penerapan / Diterapkan Sebagian
5.40	III	3	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	Dalam Penerapan / Diterapkan Sebagian
5.41	III	3	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud,* termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	Dalam Penerapan / Diterapkan Sebagian
#			**Pengamanan Fisik**	
5.42	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Dalam Penerapan / Diterapkan Sebagian
5.43	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Dalam Penerapan / Diterapkan Sebagian
5.44	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Dalam Penerapan / Diterapkan Sebagian
5.45	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Dalam Penerapan / Diterapkan Sebagian
5.46	II	1	Apakah infrastruktur komputasi yang terpasang dapat dipantau melalui CCTV ?	Dalam Penerapan / Diterapkan Sebagian
5.47	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Dalam Perencanaan
5.48	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Dalam Penerapan / Diterapkan Sebagian
5.49	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Dalam Penerapan / Diterapkan Sebagian
5.50	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Penerapan / Diterapkan Sebagian
5.51	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Perencanaan
5.52	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Dalam Penerapan / Diterapkan Sebagian
5.53	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Dalam Penerapan / Diterapkan Sebagian
			Total Nilai Evaluasi Pengelolaan Aset	**120**

Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pengamanan Teknologi**	
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Dalam Penerapan / Diterapkan Sebagian
6.4	III	2	Apakah tersedia proses pengelolaan konfigurasi perangkat komputasi (server, perangkat jaringan, sistem operasi dan aplikasi) yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh
6.5	IV	3	Apakah perangkat komputasi terpasang tersebut sudah dikaji ulang secara berkala sesuai dengan konfigurasi standard untuk keamanan sistem, dipantau efektivitasnya dan dimutakhirkan/disesuaikan konfigurasnyai melalui proses Manajemen Perubahan (*change management*)?	Diterapkan Secara Menyeluruh
6.6	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Penerapan / Diterapkan Sebagian
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Dalam Penerapan / Diterapkan Sebagian
6.8	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada **dan efektivitas keamanannya**?	Diterapkan Secara Menyeluruh
6.9	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Penerapan / Diterapkan Sebagian
6.10	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Dalam Penerapan / Diterapkan Sebagian
6.11	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Perencanaan
			"[Catatan Periksa] Minimal yang harus di log adalah sbb : 1. outbound and inbound trafik jaringan; 2. Akses terhadap sistem, server, perangkat jaringan, aplikasi kritis ; 3. penggunaan file sistem dan konfigurasi jaringan ; 4. dari perangkat keamaanan [spt. antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, data leakage prevention]; 5. event log yang berhubungan dengan sistem dan aktifitas jaringan; "	
6.12	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Dalam Penerapan / Diterapkan Sebagian
6.13	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Diterapkan Secara Menyeluruh
6.14	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Penerapan / Diterapkan Sebagian
6.15	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Dalam Perencanaan
6.16	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Dalam Penerapan / Diterapkan Sebagian
6.17	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Dalam Penerapan / Diterapkan Sebagian
6.18	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Dalam Penerapan / Diterapkan Sebagian
6.19	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian
6.20	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian
6.21	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh
6.22	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Dalam Perencanaan
6.23	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Penerapan / Diterapkan Sebagian
6.24	III	2	Apakah instansi/perusahaan anda secara rutin menganalisa dan menetapkan website yang membahayakan perusahaan atau tidak seharusnya diakses karyawan? Untuk selanjutnya website tersebut diblok agar tidak dapat diakses.	Dalam Penerapan / Diterapkan Sebagian
6.25	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagian
6.26	III	2	Apakah instansi/perusahaan anda sudah menetapkan prinsip pengembangan aplikasi yang aman (*secure coding*) yang digunakan untuk pengembangan aplikasi secara internal (*in-house*) maupun yang melibatkan pihak eksternal? misal: menggunakan standard OWASP 10	Dalam Perencanaan
6.27	III	2	Apakah instansi/perusahaan anda sudah menerapkan proses perencanaan pengembangan sistem? (Dengan mempertimbangkan hasil pemrograman yang tidak baik/laik pada sistem sebelumnya, konfigurasi *software development tool* yang aman (*secure*), kontrol terhadap lingkungan pengembangan, desain arsitektur yang aman)	Dalam Penerapan / Diterapkan Sebagian

Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
6.28	III	2	Apakah instansi/perusahaan anda menerapkan proses *source code review* (baik secara manual atau menggunakan piranti lunak) sebelum dijalankan di lingkungan produksi?	Dalam Perencanaan
6.29	II	1	Apakah instansi/perusahaan anda menerapkan kontrol akses untuk *source code* apliksi ?	Dalam Perencanaan
6.30	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Dalam Penerapan / Diterapkan Sebagian
6.31	III	3	Apakah instansi/perusahaan anda secara rutin menganalisa dan memperbaiki jika ditemukenali ancaman baru (misal adanya laporan kelemahan dan/atau teknik eksploit baru) yang berdampak pada keamanan sistem aplikasi?	Dalam Penerapan / Diterapkan Sebagian
6.32	III	3	Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	Dalam Perencanaan
6.33	III	3	Apakah instansi/perusahaan sudah menerapkan proses atau mekanisme untuk mencegah terungkapnya informasi sensitif ke luar dari perusahaan (misal membatasi/mengkarantina lampiran email atau memblokir pengiriman dokumen/data ke luar) ?	Dalam Penerapan / Diterapkan Sebagian
6.34	IV	3	Apakah instansi/perusahaan sudah menerapkan teknologi (DLP Data Leakage Prevention) untuk mencegah terungkapnya informasi sensitif ke luar dari perusahaan ?	Dalam Perencanaan
6.35	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**113**

Bagian VII: Pelindungan Data Pribadi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penerapan kontrol keamanan terkait Pelindungan Data Pribadi (PDP).

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pelindungan Data Pribadi**	
7.1	II	1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	Dalam Penerapan / Diterapkan Sebagian
7.2	II	1	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	Dalam Penerapan / Diterapkan Sebagian
7.3	II	1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	Dalam Penerapan / Diterapkan Sebagian
7.4	II	1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Pelindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian
7.5	II	2	Apakah instansi/perusahaan sudah menunjuk fungsi/unit Pejabat Pelindung Data Pribadi yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Pelindungan Data Pribadi?	Dalam Penerapan / Diterapkan Sebagian
7.6	II	2	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	Dalam Penerapan / Diterapkan Sebagian
7.7	III	2	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Pelindungan Data Pribadi?	Dalam Perencanaan
7.8	III	2	Apakah mekanisme pelindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	Dalam Perencanaan
7.9	III	2	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan	Dalam Penerapan / Diterapkan Sebagian
7.10	III	2	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?	Dalam Perencanaan
7.11	III	2	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	Dalam Perencanaan
7.12	III	2	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	Dalam Perencanaan
7.13	III	2	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	Dalam Perencanaan
7.14	III	2	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	Tidak Dilakukan
7.15	III	2	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?	Tidak Dilakukan
7.16	III	2	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	Tidak Dilakukan
			Total Nilai Evaluasi Pelindungan Data Pribadi	**32**

Bagian VIII: Suplemen

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penerapan mekanisme keamanan terkait risiko keterlibatan pihak ketiga eksternal dalam operasional penyelenggaraan layanan instansi/perusahaan

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**	
8.1			**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**	
8.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Dalam Penerapan / Diterapkan Sebagian
8.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Tidak Dilakukan
8.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Tidak Dilakukan
8.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Tidak Dilakukan
8.1.5		1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	Tidak Dilakukan
8.1.6		1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Tidak Dilakukan
8.1.7		1	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	Tidak Dilakukan
8.2			**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**	
8.2.1		1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	Tidak Dilakukan
8.2.2		1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Tidak Dilakukan
8.2.3		1	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	Tidak Dilakukan
8.3			**Pengelolaan Layanan dan Keamanan Pihak Ketiga**	
8.3.1		1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	Tidak Dilakukan
8.3.2		1	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	Tidak Dilakukan
8.3.3		1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	Tidak Dilakukan
8.3.4		1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	Tidak Dilakukan
8.3.5		1	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?	Tidak Dilakukan
8.3.6		1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	Tidak Dilakukan
8.3.7		1	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	Tidak Dilakukan
8.3.8		1	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	Tidak Dilakukan
8.4			**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**	
8.4.1		1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?	Dalam Penerapan / Diterapkan Sebagia
8.4.2		1	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	Dalam Penerapan / Diterapkan Sebagian
8.5			**Penanganan Aset**	
8.5.1		1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan / penghancuran aset?	Tidak Dilakukan
8.5.2		1	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	Tidak Dilakukan

Bagian VIII: Suplemen

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penerapan mekanisme keamanan terkait risiko keterlibatan pihak ketiga eksternal dalam operasional penyelenggaraan layanan instansi/perusahaan

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
8.6			**Pengelolaan Insiden oleh Pihak Ketiga**	
8.6.1		1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	Tidak Dilakukan
8.6.2		1	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	Tidak Dilakukan
8.7			**Rencana Kelangsungan Layanan Pihak Ketiga**	
8.7.1		1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	Tidak Dilakukan
8.7.2		1	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	Tidak Dilakukan
8.7.3		1	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	Tidak Dilakukan
			Total Nilai Evaluasi Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	**7 %**

PENUTUP

Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001. Proses evaluasi dilakukan melalui sejumlah pertanyaan di beberapa area berikut:

- Kategori Sistem Elektronik yang digunakan
- Tata Kelola Keamanan Informasi
- Pengelolaan Risiko Keamanan Informasi
- Kerangka Kerja Keamanan Informasi
- Pengelolaan Aset Informasi
- Teknologi dan Keamanan Informasi
- Suplemen (Tambahan pengukuran dilakukan untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan (Cloud Service) dan Perlindungan Data Pribadi.

Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada Pimpinan Instansi. Implementasi Indeks KAMI dilakukan oleh penyelenggara layanan publik secara elektronik melalui Bimbingan Teknis, Asesmen, dan Konsultasi.

Painan, Desember 2024

PA Kepala Dinas Komunikasi dan Informatika	PPTK Program Penyelenggaraan Persandian untuk Pengaman Informasi
WENDI, S.H., M.Hum.	ISMAN, SE., M.Si.

LAMPIRAN INDEKS KAMI

DIGITAMA

WEBINAR DIGITAMA

INDEKS KAMI 5.0

JOIN FREE

10.00 - 11.30 WIB
Kamis, 31 Oktober 2024
LIVE ON:

Benefit
E-sertifikat •
Ilmu yang bermanfaat •

Guruh Prasetyo P, S.ST., M.Si (Han).
Badan Siber Sandi Negara (BSSN)

Pendaftaran: https://myspbe.id/webinardigitama

digitama.consulting digitama.consulting

DIGITAMA
Partner in Digital Transformation

digitama.consulting

No: 4486/SRT/MKT/X/2024

SERTIFIKAT

PT Digitama Sinergi Indonesia memberikan sertifikat kepada :

Yosi, SH

Sebagai Peserta Webinar Indeks KAMI 5.0

Yogyakarta, 31 October 2024

Direktur Utama

DIGITAMA
Partner in Digital Transformation

Pradiptya Setyahadi, S.Kom., M.Sc

Webinar
Indeks KAMI 5.0

Materi	Pemateri	Alokasi Jam
Indeks KAMI 5.0	Guruh Prasetyo Putro, S.ST., M.Si (Han).	3 JP

Yogyakarta, 31 October 2024

Direktur Utama

DIGITAMA
Partner in Digital Transformation

Pradiptya Setyahadi, S.Kom., M.Sc

DIGITAMA
Partner in Digital Transformation

digitama.consulting

No: 4609/SRT/MKT/X/2024

SERTIFIKAT

PT Digitama Sinergi Indonesia memberikan sertifikat kepada :

MARDHIATUL IHSANIAH

Sebagai Peserta Webinar Indeks KAMI 5.0

Yogyakarta, 31 October 2024

Direktur Utama

DIGITAMA
Partner in Digital Transformation

Pradiptya Setyabadi, S.Kom., M.Sc

Webinar
Indeks KAMI 5.0

Materi	Pemateri	Alokasi Jam
Indeks KAMI 5.0	Guruh Prasetyo Putro, S.ST., M.Si (Han).	3 JP

Yogyakarta, 31 October 2024

Direktur Utama

Pradiptya Setyabadi, S.Kom., M.Sc

Disclaimer.

"INDEKS KAMI TIDAK DITUJUKAN UNTUK MENGANALISIS KELAYAKAN ATAU EFEKTIVITAS BENTUK PENGAMANAN YANG ADA, MELAINKAN SEBAGAI PERANGKAT UNTUK MEMBERIKAN GAMBARAN KONDISI KESIAPAN KERANGKA KERJA KEAMANAN INFORMASI KEPADA PIMPINAN INSTANSI"

Update Indeks KAMI versi 5.0

Area 1 Kategorisasi SE 1.9 Dampak Dari Kegagalan Sistem Elektronik

Perbaikan formula (status: N/A) pada Area Kerangka Kerja, Aset dan Teknologi

Penambahan area PDP dan penyesuaian area Suplemen

Penambahan dan Penyesuaian Pertanyaan pada Area Kerangka Kerja, Aset dan Teknologi

Nilai Total Indeks KAMI menjadi 918

NILAI KATEGORI SISTEM ELEKTRONIK

STRATEGIS [35-50]
SE yang berisiko terhadap penyelenggaraan negara dan pertahanan keamanan negara

TINGGI [16-34]
SE yang berisiko terhadap penyelenggaraan layanan publik dengan skala terbatas (Provinsi, Kabupaten, Kota)

RENDAH [10-15]
SE yang berisiko terhadap operasional layanan yang bersifat sementara dan hanya mengganggu Sebagian kecil pengguna layanan

Tingkat Kesiapan

No.	Kategori Sistem Elektronik	Status Kesiapan	Rentang Nilai	
			Semula	Menjadi
1	Rendah	Tidak Layak	0 – 174	0 – 247
		Pemenuhan Kerangka Kerja Dasar	175 – 312	248 – 443
		Cukup Baik	313 – 535	444 – 760
		Baik	536 – 645	761 – 916
2	Tinggi	Tidak Layak	0 – 272	0 – 387
		Pemenuhan Kerangka Kerja Dasar	273 – 455	388 – 646
		Cukup Baik	456 – 583	647 – 828
		Baik	584 – 645	829 – 916
3	Strategis	Tidak Layak	0 – 333	0 – 472
		Pemenuhan Kerangka Kerja Dasar	334 – 535	473 – 760
		Cukup Baik	536 – 609	761 – 864
		Baik	610 – 645	865 – 916

Pasal 9 PBSSN 8/2020

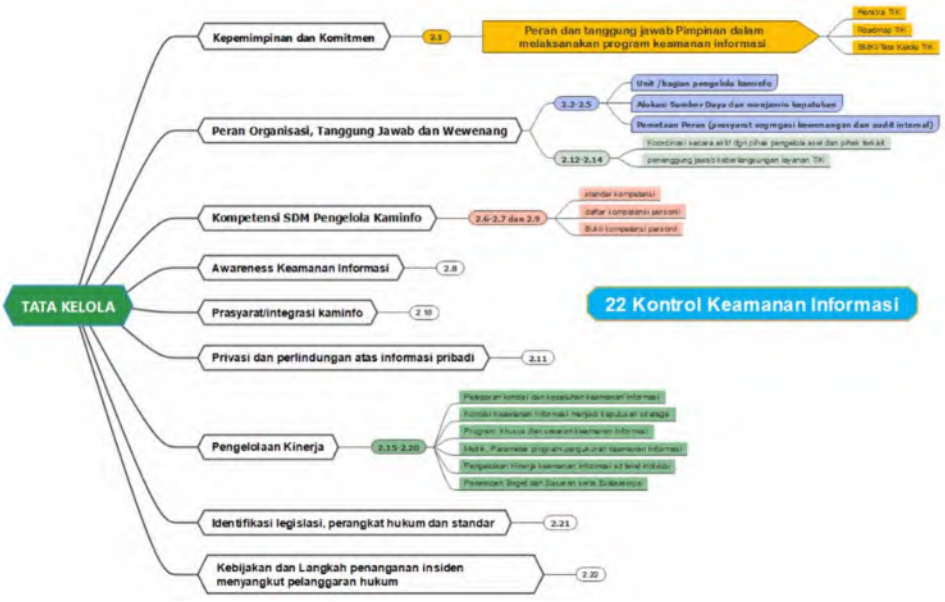
	STRATEGIS	TINGGI	RENDAH
27001	AND	AND/OR	OR
STD BSSN	AND	AND/OR	OR
STD K/L	AND	AND	N/A

KATEGORI SISTEM ELEKTRONIK (1)

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	Investasi total, termasuk belanja modal untuk sistem elektronik (misal: pengadaan sendiri, bantuan/hibah dari pusat) → • Total anggaran investasi belanja modal (t-x s.d. t). • Dokumen Laporan Realisasi Anggaran, Dokumen Kontrak, RKPD
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	Pembiayaan operasional tahunan (misal: kontrak pemeliharaan, sewa bandwidth) → • honor karyawan PPNPN atau pihak ketiga • biaya maintenance asset, lisensi
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	Kepatuhan terhadap peraturan atau standar dalam pengelolaan sistem elektronik → Regulasi Perda yang merujuk pada amanat PP 71 tahun 2019 tentang PSTE, Perpres 95, Peraturan BSSN
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	Adakah algoritma buatan Pemerintah RI yang menjadi syarat kriptografi? → • untuk LPSE, penggunaan kriptografi untuk melindungi dokumen tender yang dikirim penyedia barang/jasa • implementasi TTE
1.5	**Jumlah pengguna Sistem Elektronik** [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	Jumlah user website publik → • aplikasi milik instansi atau dinas lain yang dihosting di server

KATEGORI SISTEM ELEKTRONIK (2)

1.6	**Data pribadi yang dikelola Sistem Elektronik** [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	Data pribadi mencakup: data KK (ada nama ibu Kandung), NIP, data Kesehatan, dll. → Misal: aplikasi kepegawaian rahasia, aplikasi keuangan rahasia, aplikasi Data Rekam Medis pada OPD Dinas Kesehatan yang terhubung dengan Rumah Sakit
1.7	**Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi** [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	Data yang berhubungan dengan aset kritikal Nasional termasuk dalam kategori : Sangat Rahasia [A] →
1.8	**Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi** [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	Diukur terhadap dampak kepada layanan publik. Termasuk sistem yang servernya dititipkan di lokasi responden →
1.9	**Dampak dari kegagalan Sistem Elektronik** [A] Membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik berskala nasional atau berdampak pada layanan di sektor lain [C] Tidak tersedianya layanan publik dalam 1 propinsi atau internal 1 instansi/perusahaan	Jelas. →
1.10	**Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme)** [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	Jelas. →



DOKUMENTASI / BUKTI DUKUNG

KEBIJAKAN

Dokumen **Kebijakan keamanan informasi** (2.1), yang di dalamnya terdapat:

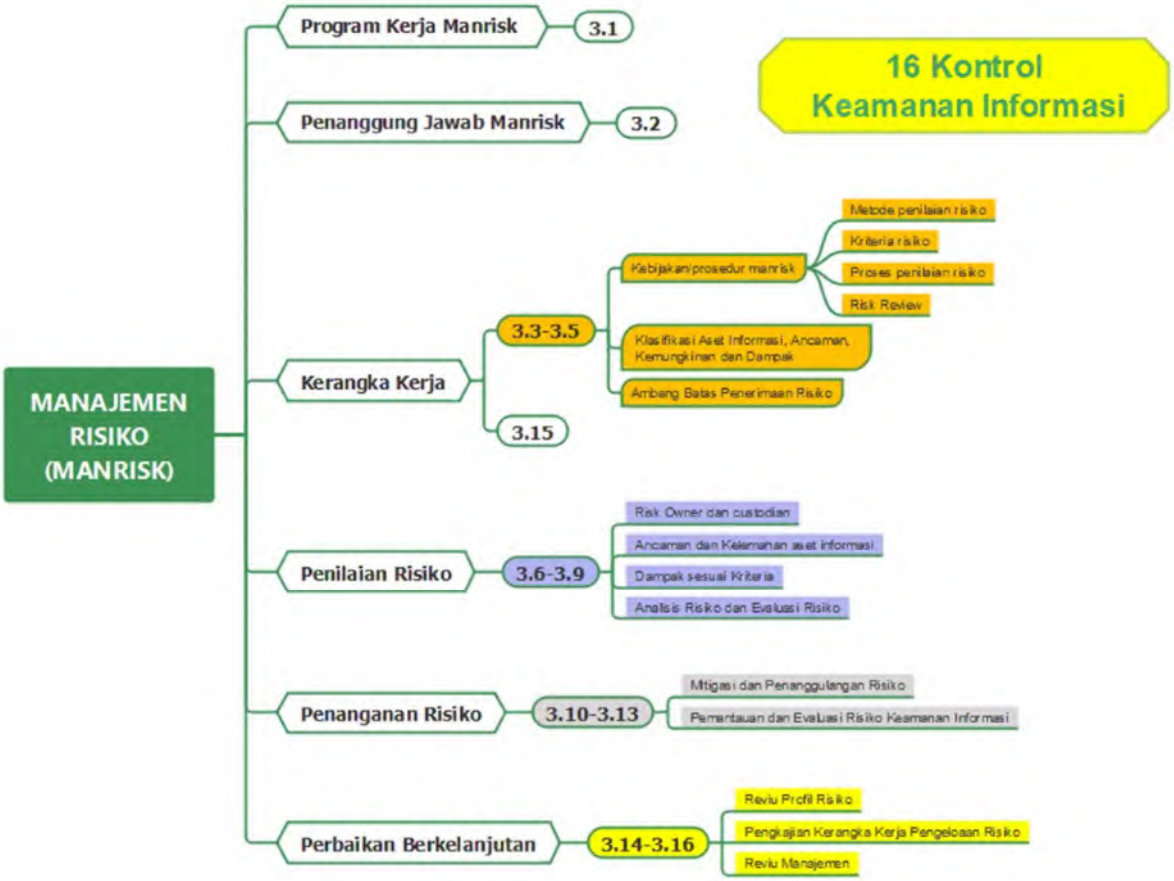
- tujuan keamanan informasi (2.1)
- unit penanggung jawab keamanan informasi disertai uraian tugas, wewenang dan tanggung jawab (2.2; 2.3; 2.5) juga mencakup koordinasi/komunikasi terkait persyaratan keamanan dg unit kerja/pihak lain (2.12)
- standar kompetensi personil (2.6)
- prosedur klasifikasi informasi dan hasil identifikasi dan klasifikasi data (termasuk data pribadi) (2.11)
- pihak internal dan eksternal yang berhubungan serta hubungannya dengan unit penanggung jawab keamanan informasi (2.12 – 2.13)
- Penanggung jawab BCP/ DRP (2.14)
- Pengukuran Kinerja SMKI termasuk metrik atau IKU, pelaporan dan evaluasinya (2.15 – 2.20)
- Pengelolaan insiden serta eskalasinya yang memerlukan tindakan hukum (2.22)

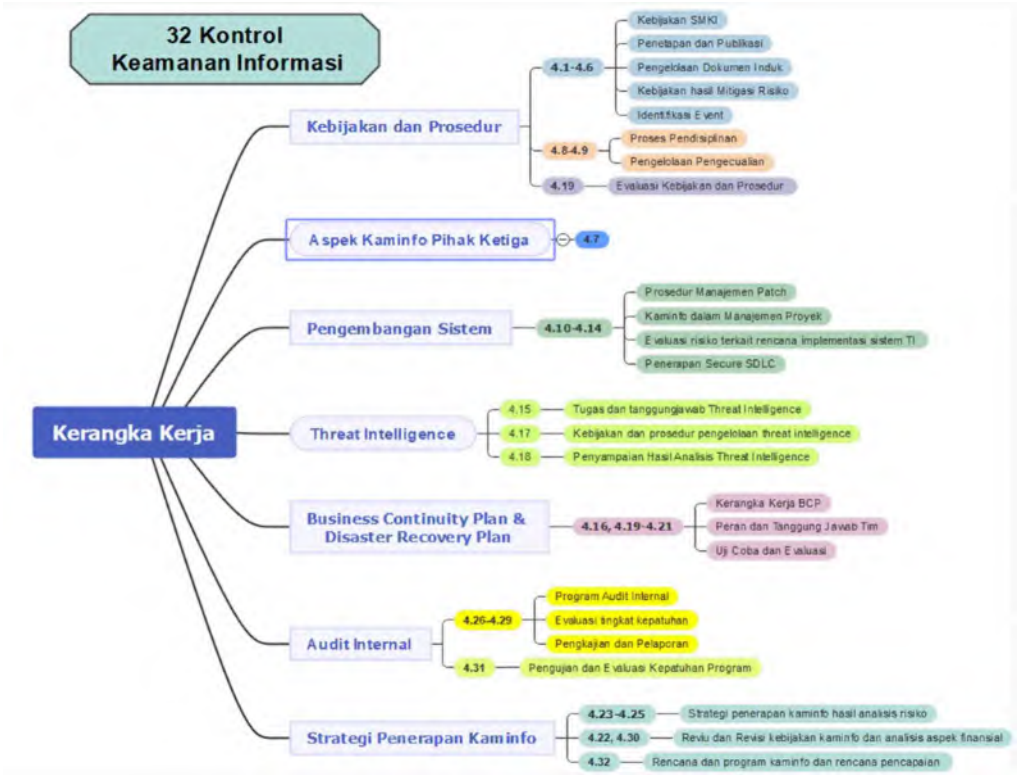
PROGRAM

- IT blue print, RPJMN/road map TI (2.1)
- Renstra/program kerja untuk pengalokasian sumber daya (2.4)
- Program peningkatan kompetensi, dan bukti kompetensi personil (2.9)
- Integrasi persyaratan keamanan dalam proses kerja misal: penghapusan aset dalam bentuk disk yang dilepas sudah mempertimbangkan data di dalamnya dengan menghapus secara logic terlebih dahulu sebelum dibuang/dihancurkan (2.10)
- Bukti penyusunan program tahun berikutnya sudah memperhatikan pengelolaan risiko (2.16)

IMPLEMENTASI

- SK Pengangkatan Unit Penanggung Jawab Keamanan Informasi (2.2 - 2.3), (2.5)
- Bukti kompetensi personil dan gap kompetensi (2.7)
- Bukti sosialisasi SMKI (2.8)
- Bukti komunikasi dapat berupa rapat atau dokumentasi persuratan (2.12 - 2.13)
- Laporan berkala implementasi/progres SMKI dan monitoring evaluasi (monev) termasuk tindak lanjut audit dan penanganan risiko pada pimpinan (2.15-2.20)
- Daftar undang-undang, regulasi, peraturan, standar keamanan informasi yang harus dipatuhi (2.21)





DOKUMENTASI / BUKTI DUKUNG

KEBIJAKAN

Dokumen Kebijakan keamanan informasi (2.1), yang di dalamnya terdapat:

- Tujuan keamanan informasi (4.1)
- Unit penanggung jawab keamanan informasi disertai uraian tugas, wewenang, dan tanggung jawab (4.1) juga mencakup koordinasi/komunikasi dengan pihak ketiga (4.4)
- Prosedur pengelolaan dokumen (4.3)
- Prosedur identifikasi event dan bagaimana ditetapkannya sebagai insiden kemudian penyelesaiannya/recovery dan lesson learn nya (4.6)
- Dokumen kebijakan terkait sanksi pelanggaran keamanan informasi atau aturan kepegawaian atau NDA (4.8)
- Dokumen kebijakan yang memuat di dalamnya pengecualian (4.9)

PROGRAM

- Prosedur patch manajemen (4.10)
- Formulir evaluasi rencana pengadaan/implementasi sistem TI (4.12)
- Prosedur, flowchart sampai penerapan tentang secure
- Penerapan Secure SDLC (4.13)
- Prosedur BCP/DRP mulai dari perencanaan,
- Kewenangan Tugas pemantauan ops/threat intel, kebijakan/prosedur dan pelaporan (4.15, 4.17-4.18))
- Dokumen BCP, RTO dan RPO, uji cuba BCP (4.16, 4.19-21)
- implementasi, reviu dan evaluasi (4.15 - 4.18)
- Pengukuran kinerja SMKI termasuk metrik atau IKU, pelaporan dan evaluasinya (4.23)
- Prosedur terkait audit internal dan programnya (4.26 - 4.29)
- Roadmap, cascading, RKA sesuai roadmap dan laporan tahunan (4.32)

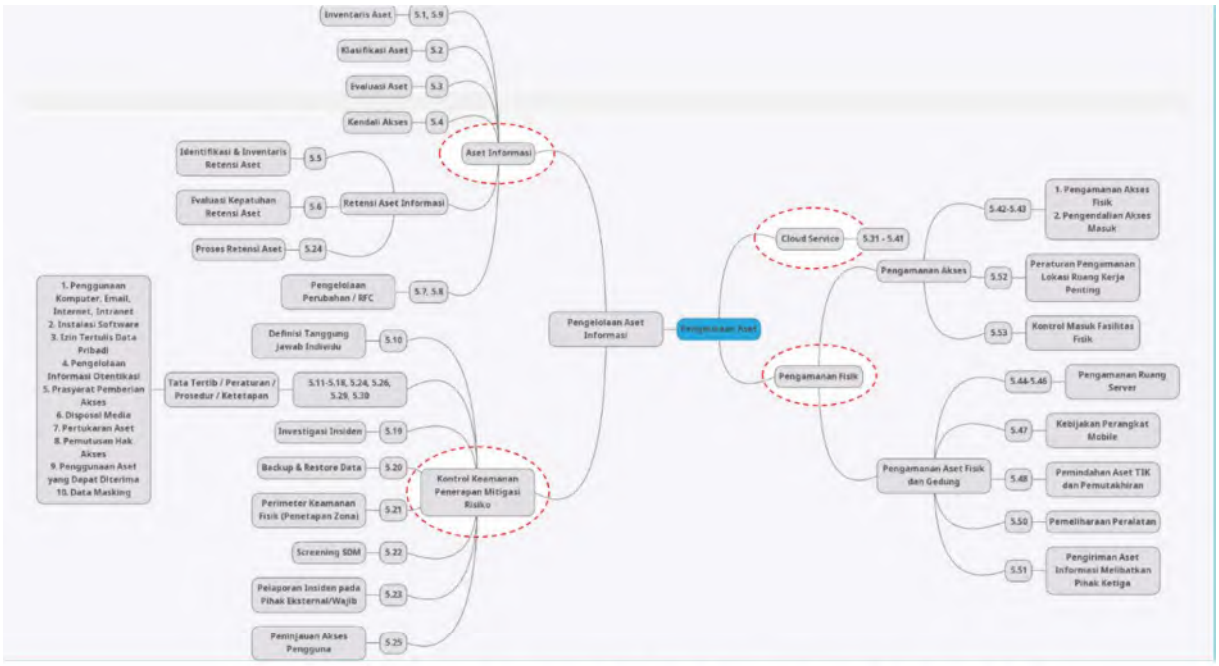
IMPLEMENTASI

- Bukti publikasi kebijakan berupa portal atau Surat
- Edaran atau bukti sosialisasi (4.2)
- Dokumen Risk Register (4.5)
- Dokumen kontrak dengan pihak ketiga termasuk NDA, pengaturan hak akses, pengamanan data penting (4.7, 4.11)
- Laporan maintenance (4.14)
- Daftar undang-undang, regulasi, peraturan, standar keamanan informasi yang harus dipatuhi , Berita Acara Hasil Reviu (4.30)
- dokumen profil risiko (4,23, 4.24)
- Program kerja (4.25)
- Notula/Laporan/Hasil Analisa/Undangan/Bukti Rapat (4.30)

Tujuan

Mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

Aset Informasi	5.1-5.4, 5.7-5.9
Retensi Aset Informasi	5.5-5.6, 5.24
Kontrol Keamanan Penerapan Mitigasi Risiko	5.10-5.23, 5.25-5.28, 5.30
Data Masking	5.29
Pengamanan Layanan Infrastruktur Awan (Cloud Service)	5.31-5.41
Pengamanan Akses	5.42-5.43, 5.52-5.53
Pengamanan Aset Fisik dan Gedung	5.44-5.51



DOKUMENTASI / BUKTI DUKUNG

KEBIJAKAN

Dokumen Kebijakan keamanan informasi (2.1), yang di dalamnya terdapat:

- **Definisi Klasifikasi Aset Informasi (5.2)**
- **Klasifikasi Aset Informasi sesuai tingkat kepentingan serta evaluasi dan proses pengamanannya (5.3)**
- **Prosedur Manajemen Perubahan (5.7) dan Prosedur Release Management (5.9)**
- **Prosedur Pengelolaan Konfigurasi (5.8)**
- **Kebijakan/ketentuan penggunaan komputer, email, internet dan intranet (5.11)**
- **Kebijakan/ketentuan pengamanan dan penggunaan aset terkait HAKI (5.12)**
- **Kebijakan terkait instalasi piranti lunak di aset TI (5.13)**
- **Kebijakan/ketentuan terkait penggunaan data pribadi (5.14)**
- **Prosedur pengelolaan identitas elektronik dan proses otentikasi serta pelanggarannya (5.15)**
- **Prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi (5.16)**
- **Kebijakan/ketentuan terkait waktu penyimpanan untuk klasifikasi data dan syarat penghancuran data (5.17)**
- **Kebijakan/ketentuan terkait pertukaran data dengan pihak eksternal termasuk pelaporan insiden keamanan informasi (5.18 dan 5.23)**
- **Prosedur back up restore dan bukti (5.20)**
- **Ketentuan terkait pengamanan fisik beserta definisi zona dan klasifikasi aset di dalamnya (5.21)**
- **Prosedur penghancuran data (5.24)**
- **Prosedur penggunaan akses dan Langkah pembenahan apabila terjadi ketidak sesuaian terhadap kebijakan yang berlaku (5.25)**
- **Prosedur terkait SDM yang mutasi/keluar dan tenaga kontrak/outsource yang habis masa Kerja (5.25)**
- **Prosedur penggunaan perangkat informasi milik pihak ketiga (5.29)**

IMPLEMENTASI

- **Daftar aset informasi (5.1), Daftar klasifikasi informasi (5.3), Dokumen akses kontrol (5.4), dan Daftar data/informasi yang harus dibackup (5.27)**
- **Bukti implementasi proses pengelolaan perubahan terhadap sistem, proses Bisnis dan proses TI (5.7)**
- **Bukti penyidikan/investigasi penyelesaian insiden (5.19)**
- **Bukti laporan analisa kepatuhan procedure backup (5.27)**
- **Bukti daftar penerapan keamanan : laporan, formulir yang telah diisi (5.28)**
- **Laporan penilaian risiko (5.31)**
- **Dokumen klasifikasi data (5.32)**
- **Laporan identifikasi kebutuhan cloud service (5.34)**
- **Laporan evaluasi (5.35)**
- **Kebijakan SMKI (5.36)**
- **Kebijakan BCP (5.38)**
- **SOP Penanganan Insiden (5.39)**
- **SOP Pengelolaan Data (5.40)**

Tujuan

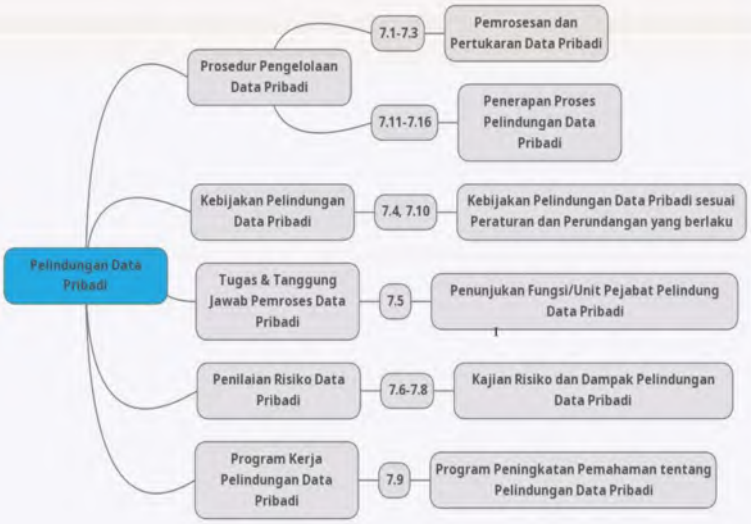
Mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

Keamanan Data	6.12,6.13, 6.14, 6.33, 6.34
Keamanan Jaringan	6.1, 6.2
Keamanan Sistem dan Aplikasi	6.7, 6.21, 6.24
Secure Development	6.26-6.29
Manajemen Konfigurasi	6.3, 6.4, 6.5, 6.20, 6.25
Manajemen Akses	6.15-6.19
Sistem Monitoring	6.8, 6.9, 6.10, 6.11, 6.22, 6.23
Pengujian Keamanan	6.6, 6.30, 6.31, 6.32, 6.35

Tujuan

Mengevaluasi kelengkapan, konsistensi dan efektifitas penerapan kontrol keamanan terkait Pelindungan Data Pribadi (PDP).

Prosedur Pengelolaan Data Pribadi	7.1-7.3, 7.11-7.16
Kebijakan Pelindungan Data Pribadi	7.4, 7.10
Tugas & Tanggung Jawab Pemroses Data Pribadi	7.5
Penilaian Risiko Data Pribadi	7.6-7.8
Program Kerja Pelindungan Data Pribadi	7.9



DOKUMENTASI / BUKTI DUKUNG

KEBIJAKAN

- Kebijakan Privasi / Pelindungan Data Pribadi (7.4 dan 7.10, 7.16)
- SK Pelindung Data Pribadi (7.5)

PROGRAM

- Prosedur / SOP Pengelolaan Data (7.2, 7.12)
- Prosedur / SOP Penanganan Insiden (7.11)
- Prosedur / SOP Verifikasi Pengguna (7.13)
- Prosedur / SOP Penghapusan Data (7.14, 7.15)

IMPLEMENTASI

- Dokumen Klasifikasi Data Pribadi, ROPA (7.1)
- Dokumentasi Pemrosesan Data Pribadi (7.3)
- Laporan Insiden Kebocoran Data (7.6)
- Laporan Penilaian Risiko (7.7)
- Laporan Evaluasi (7.8)
- Laporan Literasi/Sosialisasi Pelindungan Data Pribadi (7.9)

Tujuan

Mengevaluasi kelengkapan, konsistensi dan efektivitas penerapan mekanisme keamanan terkait risiko keterlibatan pihak ketiga eksternal dalam operasional penyelenggaraan layanan instansi/perusahaan

Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga	8.1 (7 Kontrol)
Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga	8.2 (3 Kontrol)
Pengelolaan Layanan dan Keamanan Pihak Ketiga	8.3 (8 Kontrol)
Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga	8.4 (2 Kontrol)
Penanganan Aset	8.5 (2 Kontrol)
Pengelolaan Insiden oleh Pihak Ketiga	8.6 (2 Kontrol)
Rencana Kelangsungan Layanan Pihak Ketiga	8.7 (3 Kontrol)

Diskusi..

Guruh Prasetyo Putro
0857 1030 8907