Indeks Keamanan Informasi (IKAMI)

Direktorat Kamsibersan Pemerintah Daerah, Badan Siber dan Sandi Negara

Agenda

- Sesi-1
  - Keamanan Informasi dan Sistem Manejemen Keamanan Informasi
  - Indeks Keamanan Informasi (Indeks KAMI)
- Sesi-2
  - Area Indeks KAMI & Praktik Pengisian Instrumen Indeks KAMI v.4.2 rev-3

Sesi-1

- Keamanan Informasi dan Sistem Manejemen Keamanan Informasi
- Indeks Keamanan Informasi (Indeks KAMI)

Keamanan Informasi

Risiko Keamanan Informasi

Risiko Hukum	Risiko Finansial	Risiko Reputasi	Risiko Operasional
Dampak hukum dari gagalnya keamanan informasi di organisasi (Kesalahan pengelolaan atau kebocoran data pribadi pelanggan)	Dampak dari kerugian finansial akibat fraud (Unauthorized people dapat melakukan transaksi yang sah)	Dampak reputasi terjadinya insiden keamanan informasi di Organisasi (Website terkena deface)	Dampak pada layanan dari terjadinya gangguan (ketersediaan, keutuhan, kerahasiaan) keamanan informasi (Layanan Sistem Informasi tidak berjalan selama sekian jam)

Apa itu INFORMASI ?

INFORMASI adalah data yang telah diolah menjadi bentuk yang memiliki arti bagi si penerima dan bermanfaat bagi pengambilan keputusan saat ini atau mendatang

(Raymond Mcleod jr, *Information Security Management*)

INFORMASI ELEKTRONIK adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (Electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

(UU 11/2008 tentang ITE)

"Informasi dibuat, diterima dan dipelihara sebagai BUKTI dan sebagai ASET oleh seseorang maupun organisasi, dalam memenuhi kewajiban hukum atau dalam transaksi Bisnis.",

(ISO 15489-1:2016 *Information and Documentation* – Record Managements)

Aset Informasi

Segala sesuatu yang memiliki nilai bagi organisasi dan oleh karenanya harus dilindungi, dikelola, diberi klasifikasi, analisis dan mitigasi risiko.

Perangkat Lunak

Aplikasi (Misal : Aplikasi E-procurment, E-commerce, Fintek, Sistem Operasi, MS Office, Software Antivirus, Tool/Software Monitoring, dsb)

Perangkat Keras

PC/Laptop, Server, Router, Kabel LAN, Modem, Storage, Flash Disk, dsb.

Dokumen/ Data

Dokumen Penawaran Penyedia, Data Penyedia, Kebijakan Dan Prosedur TI, Konfigurasi LAN, Hasi Pengkajian Risiko (Risk Register), Hasil , Audit Log, Hasil Monitoring Penggunaan Bandwidth Jaringan, dsb.

Sarana/Prasarana

Sumber Daya Listrik PLN, UPS, Genset, A/C, CCTV, Alat Pemadam Kebakaran, Alat Pengukur Suhu dan Kelembaban, dsb.

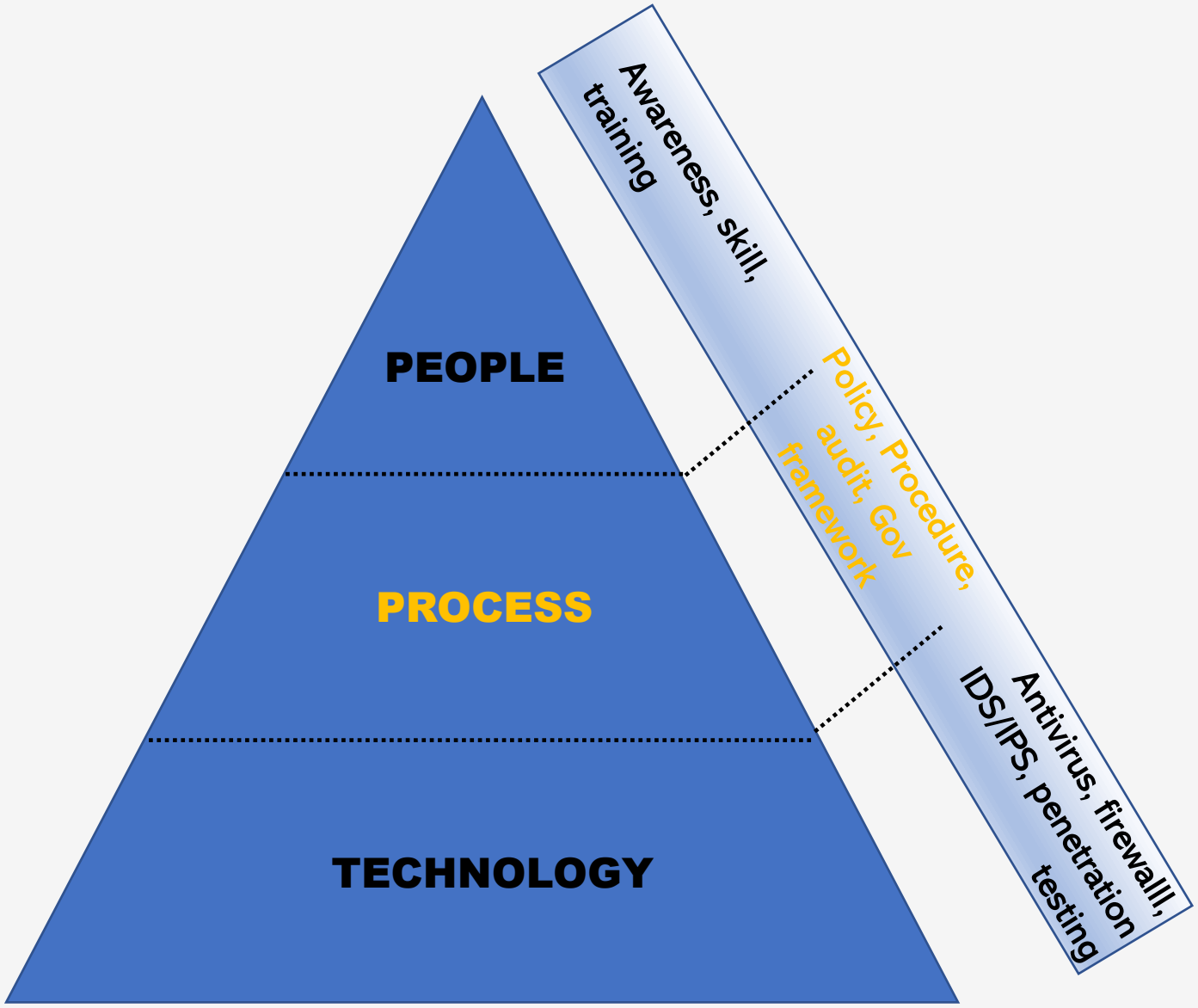
SDM/Vendor

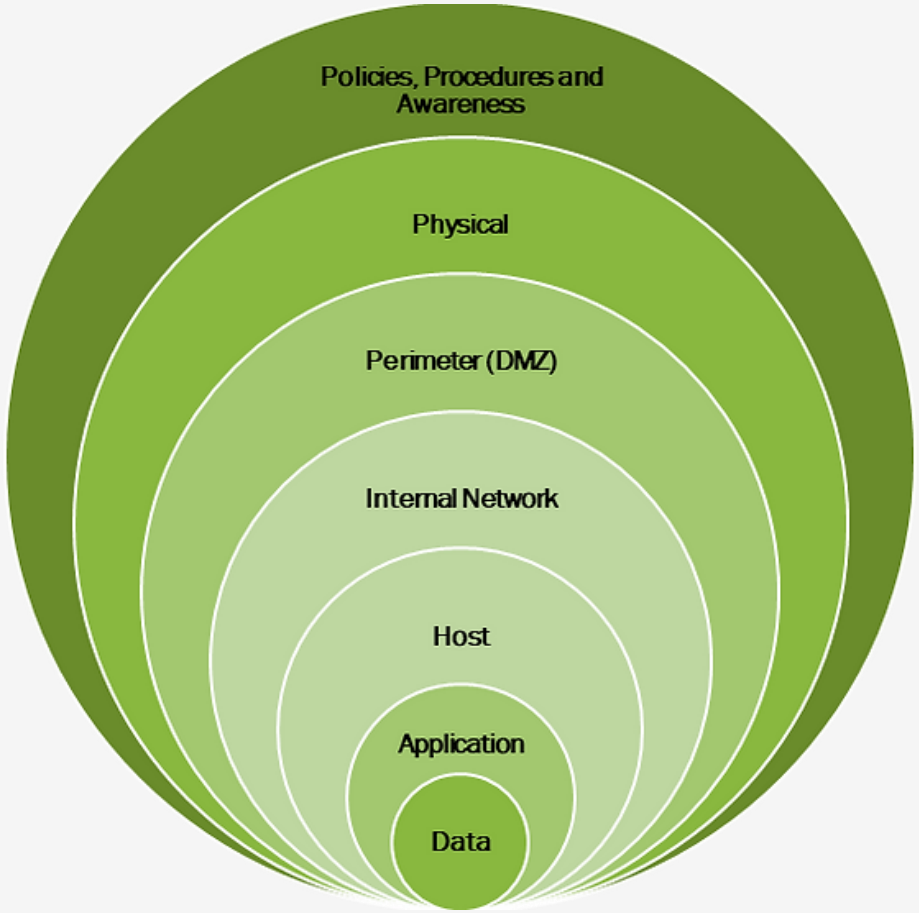
System Administrator, Pengembang (*Programmer*) dan Penyedia Jasa (Vendor/ Supplier)

Sistem Manajemen Keamanan Informasi

(SMKI)

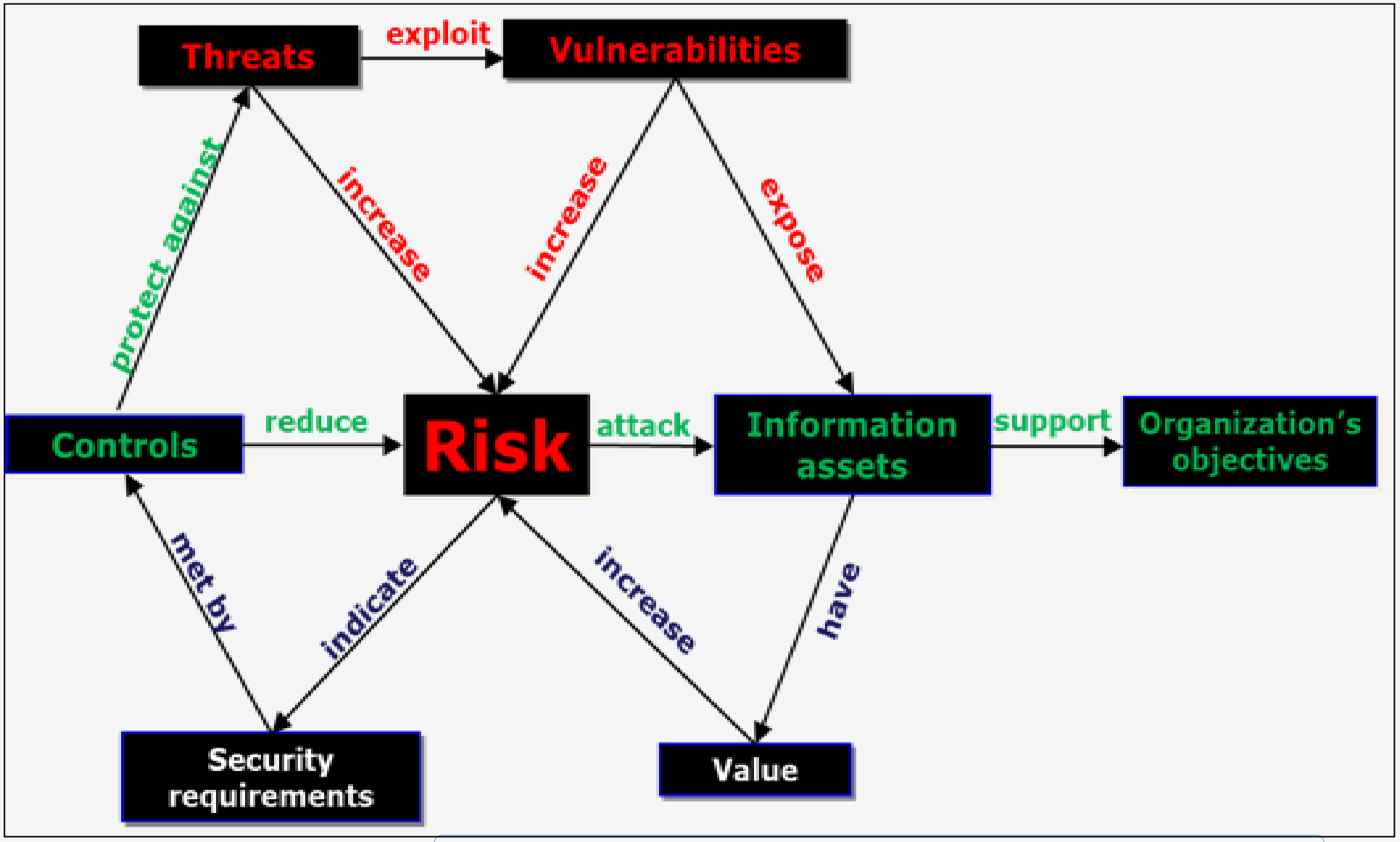
Pilar Keamanan Informasi





Layers on Defense in Depth

Apa itu Risiko ?



Risiko adalah kemungkinan sebuah Ancaman (threat) menyerang kerawanan (vulnerability) pada sebuah aset informasi.

Ref: ISO/IEC 27002

Apa itu SMKI ?

Information Security Management System (ISMS) atau SMKI merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (Plan), mengimplementasikan dan mengoperasikan (Do), memonitor dan meninjau ulang (Check) serta memelihara dan meningkatkan atau mengembangkan (Act) terhadap keamanan informasi perusahaan.

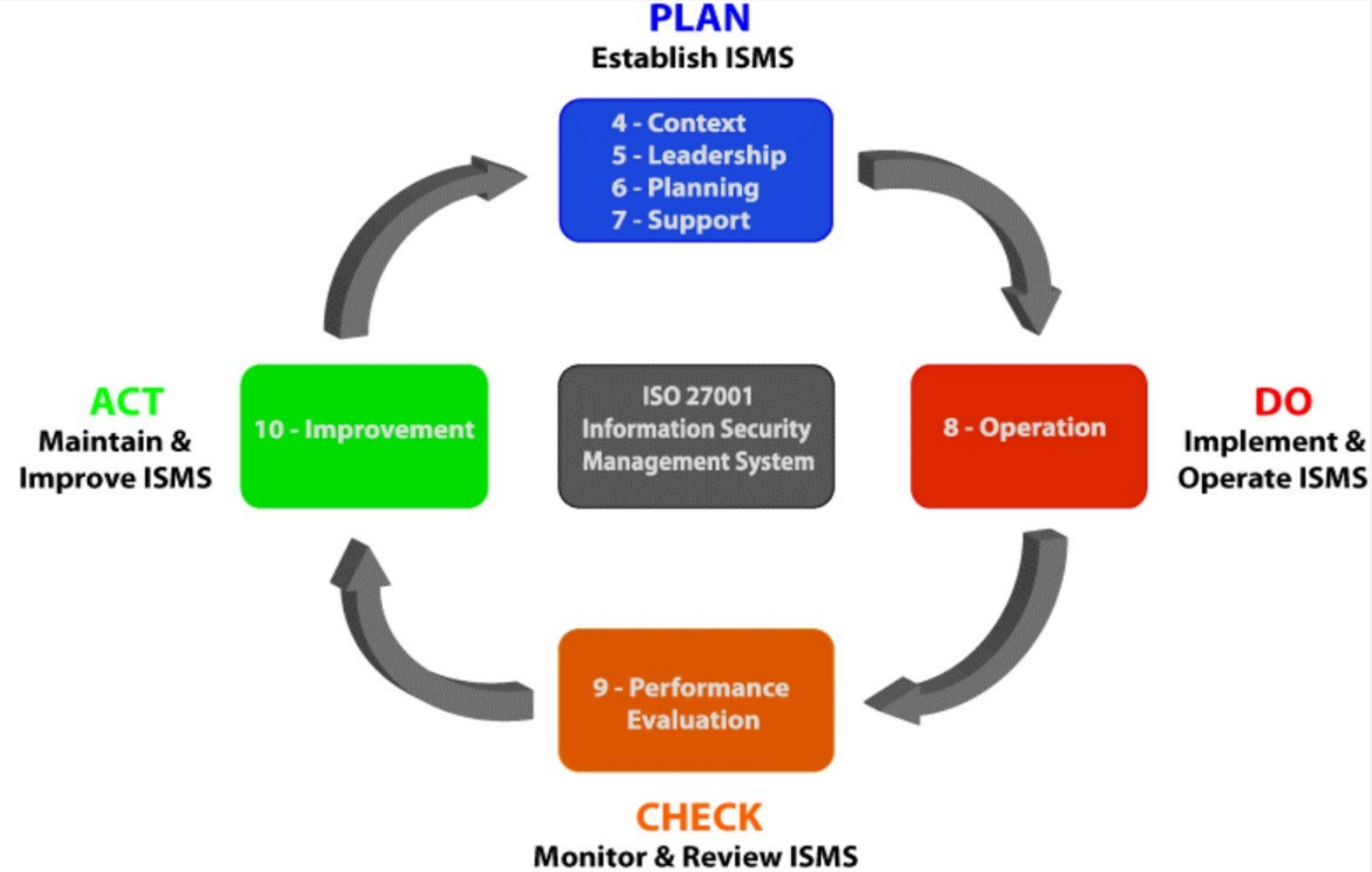
(SNI ISO/IEC 27001:2013)

Tujuan Penerapan SMKI

Untuk menjaga :

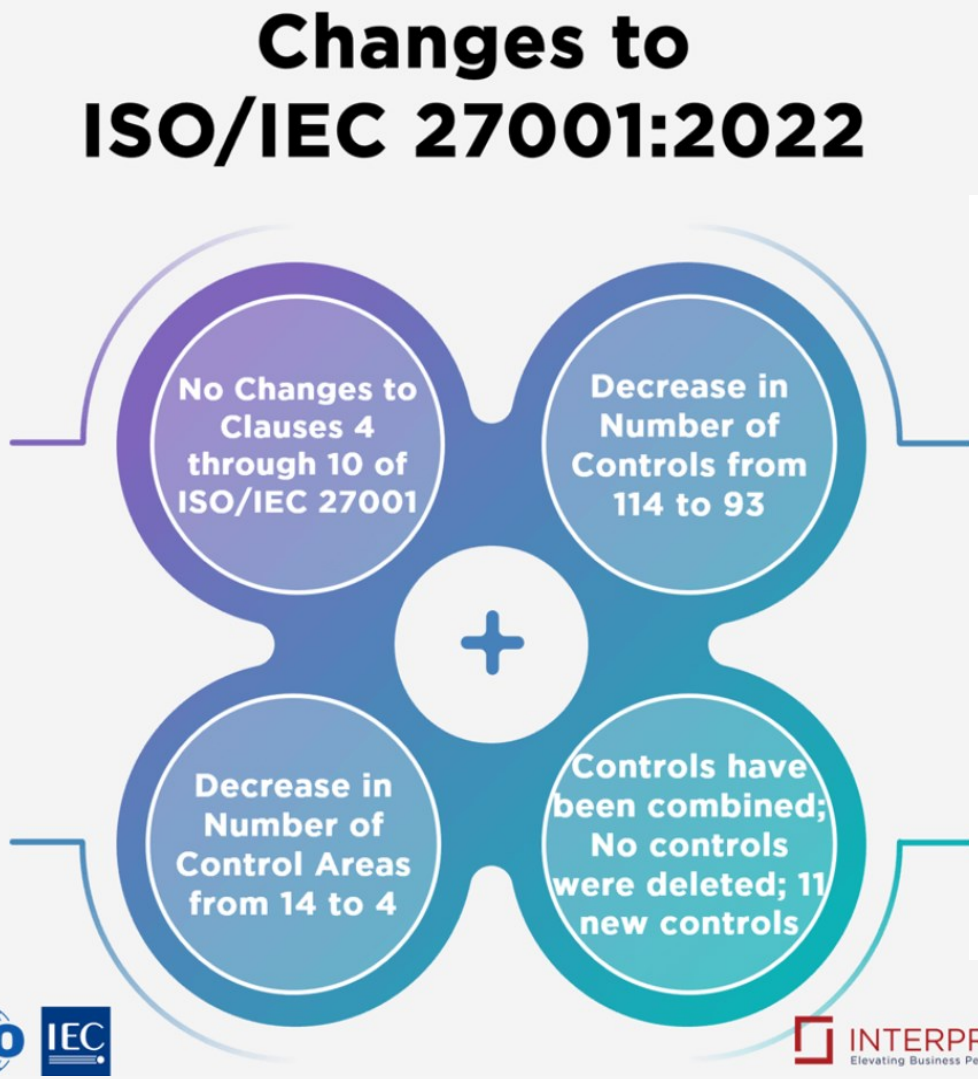
- Kerahasiaan (*Confidentiality*), menjamin bahwa hanya mereka yang memiliki hak yang dapat mengakses informasi tertentu.
- Integritas (*Integrity*), menjamin kelengkapan informasi dan menjaga kerusakan atau ancaman yang mengakibatkan berubah informasi dari aslinya.
- Ketersediaan (*Availability*), pengguna yang berwenang memiliki akses ke informasi tanpa adanya gangguan/hambatan.

Model PDCA dalam SNI ISO/IEC 27001:2013



Sumber: http://netgrowthltd.co.uk/ISO27001.aspx

Main changes in ISO 27001: 2022



Sumber: https://advisera.com/27001academy

SNI ISO:IEC 27001:2013 (1/2)

Ruang lingkup :

1. Scope
2. Normative References
3. Term & Condition

No	Klausul	Persyaratan
4	Konteks Organisasi	❖ Memahami organisasi dan konteksnya ❖ Memahami kebutuhan dan harapan dari pihak yang berkepentingan ❖ Penentuan ruang lingkup SMKI ❖ Sistem Manajemen Keamanan Informasi
5	Kepemimpinan / Leadership	❖ Kepemimpinan dan komitmen ❖ Kebijakan ❖ Peran, tanggungjawab dan kewenangan organisasi
6	Perencanaan	❖ Tindakan untuk menangani risiko dan peluang ❖ Sasaran keamanan informasi dan perencanaan untuk mencapainya

SNI ISO:IEC 27001:2013 (2/2)

No	Klausul	Persyaratan
7	Support	❖ Sumberdaya ❖ Kompetensi ❖ Awareness / kepedulian ❖ Komunikasi ❖ Informasi yang terdokumentasi
8	Operasional	❖ Perencanaan dan pengendalian operasional ❖ Penilaian risiko keamanan informasi ❖ Treatment terhadap risiko keamanan informasi
9	Evaluasi Kinerja	❖ Pemantauan, pengukuran, analisis, dan evaluasi ❖ Internal audit ❖ Review Manajemen
10	Peningkatan / improvement	❖ Ketidaksesuain dan Tindakan korektif ❖ Perbaikan berkelanjutan

Alur Penerapan SMKI

Contoh literasi Implementasi Keamanan Informasi

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Sumber: security.org

https://haveibeenpwned.com/

Salah satu cara cek data akun bocor

TERUS MENERUS DATA BOCOR

Belakangan heboh 1,3 miliar data Sim card milik pengguna Indonesia dijual Bjorka di breached. to. Kasus kebocoran data di indonesia bukan pertama kali.

Data IndiHome
- Beredar informasi di media sosial Twitter bahwa ada 26 juta data pelanggan IndiHome bocor dan masuk situs gelap.

Data PLN
- Lebih dari 17 juta data pelanggan PLN beredar di situs breached.to, 18 Agustus 2022.

Data SIM
- Akun atas nama Bjorka di breached. to mengklaim memiliki 1,3 miliar data registrasi SIM prabayar milik pengguna di Indonesia.

Data KPU
- Selain memiliki 1,3 miliar data SIM *card* ponsel pengguna Indonesia, Bjorka juga mengklaim memiliki 105 juta data kependudukan warga Indonesia.

Data Facebook
- Facebook dilaporkan mengalami kasus kebocoran data pribadi para penggunanya pada April 2021. Data pengguna Facebook di Indonesia dilaporkan ada 130.331 akun yang diretas.

Data BPJS
- Sebanyak 279 juta data pengguna BPJS Kesehatan dijual di situs forum online Raidforums.com seharga 0,15 bitcoin atau sekitar Rp 87,6 juta pada Mei 2021. Bahkan 20 juta data lainnya menampilkan foto pribadi.

Data BRI Life
- Data sekitar 2 juta nasabah asuransi BRI Life diduga bocor pada Juli 2021.

Data eHAC
- Sebanyak 1,3 juta data pengguna aplikasi eHAC milik Kementerian kesehatan diduga bocor, Agustus 2021.

Data KPAI
- Data-data milik KPAI pada Oktober 2021 disebar dan dijual di forum online oleh pengguna dengan nama C77.

Data Bank Jatim
- Pemilik akun bl4ckt0r mengaku memiliki database Bank Jatim sebesar 378 gigabyte. Data itu juga dijual seharga USD 250 ribu.

Data Polri
- Pemilik akun Twitter @son1x777 mengaku memiliki ribuan informasi pribadi, hingga daftar pelanggaran yang dilakukan anggota Polri juga ikut

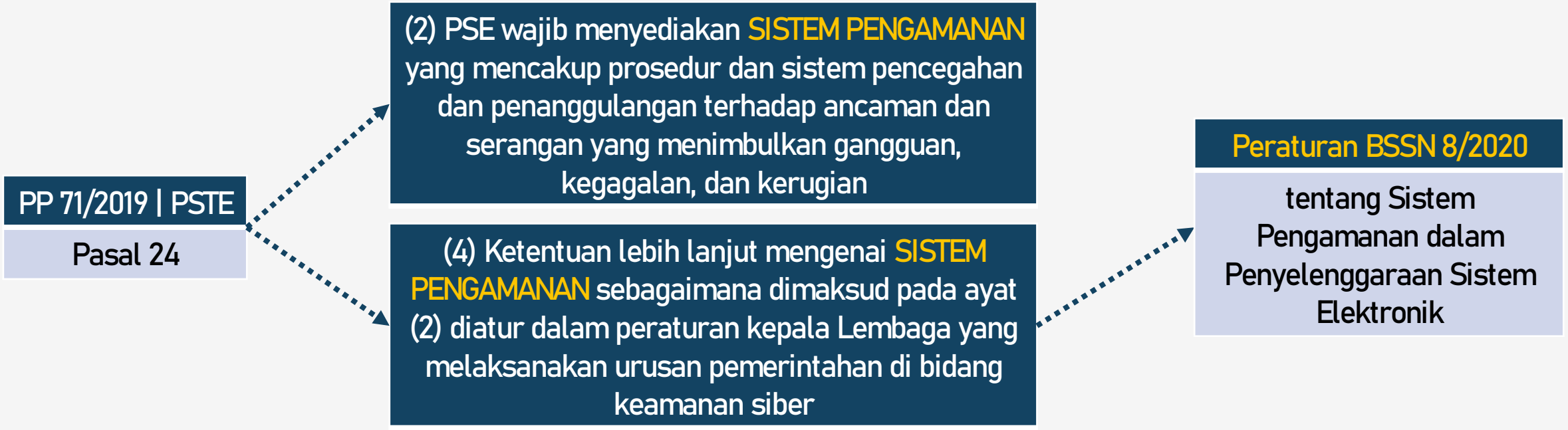
tempo.co

Naskah: Inge Klara Safitri Sumber: Diolah Tempo Ilustrasi: Freepik.com Desain: Moerat Sitompul

Dasar Hukum

UU 19/2016	Pasal 15 ayat (1) "*setiap PSE harus menyelenggarakan SE secara andal dan aman serta bertanggung jawab terhadap operasinya SE sebagaimana mestinya*"
Perpres 95/2018	Pasal 48 ayat (1) "*Manajemen keamanan informasi bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi*"
PP 71/2019	Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, pada pasal 4, 6, 12, & 13 terdapat ketentuan yang harus dipenuhi sbg PSE
Permendagri 18/2020 | 48/2021	tentang Laporan dan Evaluasi Penyelenggaraan Pemerintahan Daerah serta Perencanaan Binwas Penyelenggaraan Pemda Tahun 2022
Per.BSSN 8/2020	Tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik
Per.BSSN 8 & 9/2021	Tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 menggunakan Indeks Keamanan Informasi

Fundamental Kewajiban PSE



Disclaimer

IKAMI tidak ditujukan untuk menganalisis kelayakan/ efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi kepada pimpinan instansi

5W-1H tentang IKAMI

What ?

Alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di organisasi

Why ?

- ❑ Memberikan gambaran kondisi kesiapan kerangka kerja pengamanan informasi kepada pimpinan instansi terhadap Penerapan SNI/ISO IEC 27001
- ❑ sebagai sarana untuk meningkatkan kesadaran keamanan informasi dan peningkatan kesiapan SMKI

Who ?

PSE yang mempersiapkan penerapan SNI/ISO IEC 27001

When ?

Digunakan secara berkala sebagai alat dalam melakukan tinjauan ulang kesiapan keamanan informasi sekaligus mengukur keberhasilan inisiatif yang diterapkan

Where ?

Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang memenuhi aspek keamanan pada SNI/ISO IEC 27001

How ?

Menggunakan instrument Indeks KAMI yang dapat diunduh pada tautan :
https://bssn.go.id/indeks-kami/

Tujuan IKAMI

- Menjadi strategi peningkatan awareness bagi organisasi dalam membuat Komitmen Pimpinan dan semua unsur terkait di Organisasi
- Mempersiapkan penerapan Sistem Manajemen Keamanan Informasi berdasarkan Standar SNI ISO/IEC 27001
- Menjaga Tata Kelola Keamanan Informasi terhadap layanan kepada masyarakat yang menjadi ruang lingkup, sehingga menambah kepercayaan masyarakat dan reputasi organisasi
- Melindungi aset informasi Instansi penyelenggara layanan publik dari segala bentuk ancaman, baik internal maupun eksternal
- Mengevaluasi Penerapan Keamanan Manajemen Pihak Ketiga, Keamanan Layanan Berbasis Cloud dan Perlindungan Data Pribadi

Evolusi IKAMI

- Versi 1.0
- Rilis pertama 16-11-2008

- Versi 2.1, 2.2, 2.3
- Update definisi
- Rumus Penentuan Tingkat Kematangan

- Versi 4.2
- Perbaikan formula dan grafik.

2008 2011 2012 2015 2019 2021

- Versi 2.0
- Penggunaan Analisis Tingkat Kematangan

- Versi 3.0, 3.1
- Penggunaan Kategorisasi Sistem Elektronik
- Penyesuaian dengan perubahan kontrol di ISO/IEC 270001:2013

- Versi 4.0, 4.1
- Perubahan definisi dan istilah
- Penambahan Evaluasi Aspek Khusus (Pihak ke-3, Layanan Cloud dan Perlindungan Data Pribadi)

Posisi IKAMI dalam Per.BSSN 8/2020

Pasal 9

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

Pasal 12

Untuk mempersiapkan penerapan SNI ISO/IEC 27001 sebagaimana dimaksud dalam Pasal 9, Penyelenggara Sistem Elektronik dapat melakukan penilaian berdasarkan Indeks KAMI.

Domain Penilaian IKAMI

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

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

Suplemen digunakan untuk evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur Awan dan Perlindungan Data Pribadi. Hasil penilaian Suplemen disampaikan dalam bentuk persentase (%) dan tidak mempengaruhi tingkat kematangan.

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

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

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

Hasil Evaluasi Akhir Penilaian IKAMI

Tingkat Kesiapan

Kategori SE		Skor Akhir		Status Kesiapan
Rendah				
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi				
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis				
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

Tingkat Kematangan

I

- Perlunya Pengelolaan keamanan informasi
- Langkah pengamanan: reaktif, tidak teratur, tanpa alur komunikasi & kewenangan yg jelas
- Kelemahan Tidak teridentifikasi
- Pihak yg terlibat tidak sadar akan tanggung jawab

II

- Pengamanan mayoritas area teknis
- Belum terdokumentasi dgn baik
- Masih banyak ditemukan kelemahan dalam manajemen pengamanan
- Manajemen pengamanan belum konsisten
- Pihak yg terlibat belum memahami tanggung jawab

III

- Bentuk pengamanan sudah diterapkan secara konsisten & terdokumentasi resmi
- Dilakukan evaluasi secara berkala
- Kerangka kerja pengamanan sudah mematuhi ambang batas minimum standar
- Secara umum semua pihak sadar tanggung jawab

IV

- Pengamanan efektif Sesuai strategi manajemen risiko
- Evaluasi secara rutin, formal & terdokumentasi
- Manajemen pengamanan pro-aktif dan konsisten dalam pembenahan
- Insiden diselesaikan melalui proses formal
- Pegawai bagian tidak terpisahkan dari pengamanan informasi

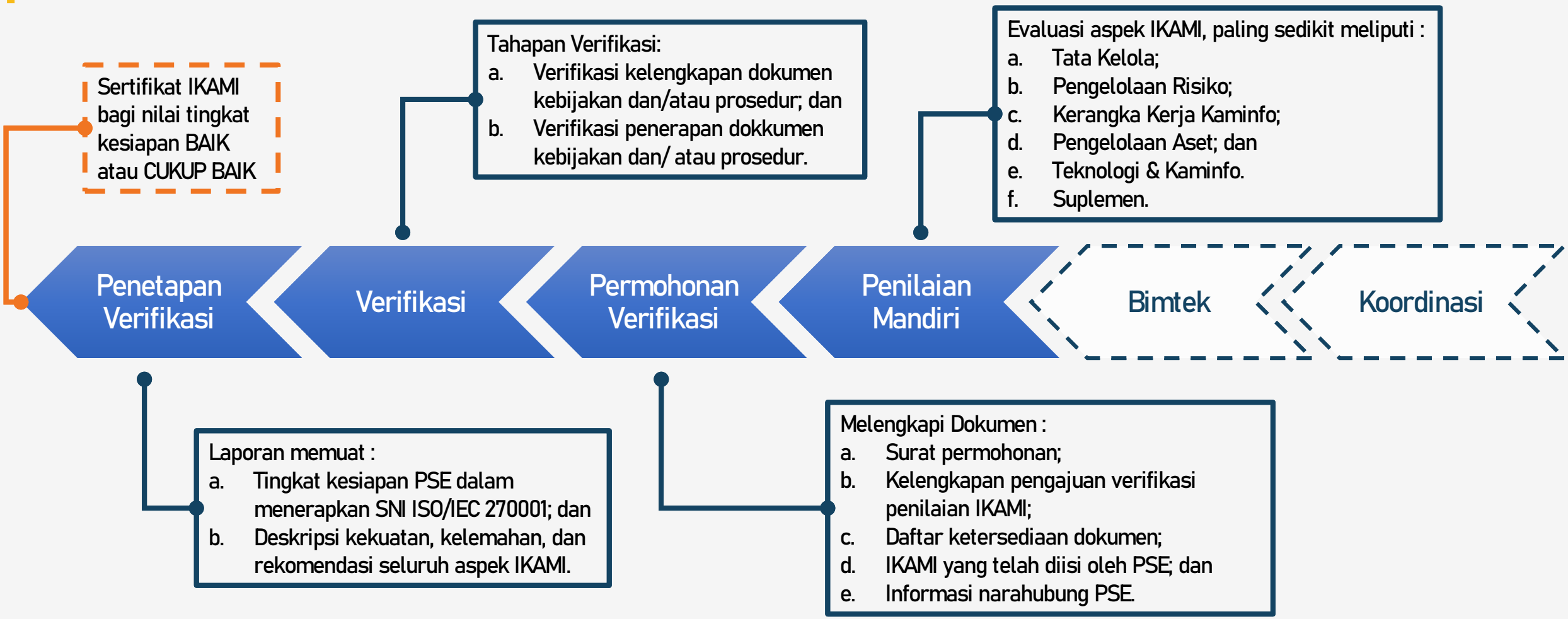
V

- Pengamanan kontinu & efektif melalui program pengelolaan risiko terstruktur
- Pengamanan informasi & manajemen risiko terintegrasi dengan tugas pokok instansi
- Kinerja pengamanan dievaluasi secara kontinu dgn analisa parameter
- Pegawai proaktif

Per.BSSN 8/2021

Tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 menggunakan Indeks Keamanan Informasi (Indeks KAMI)

Proses Penilaian IKAMI

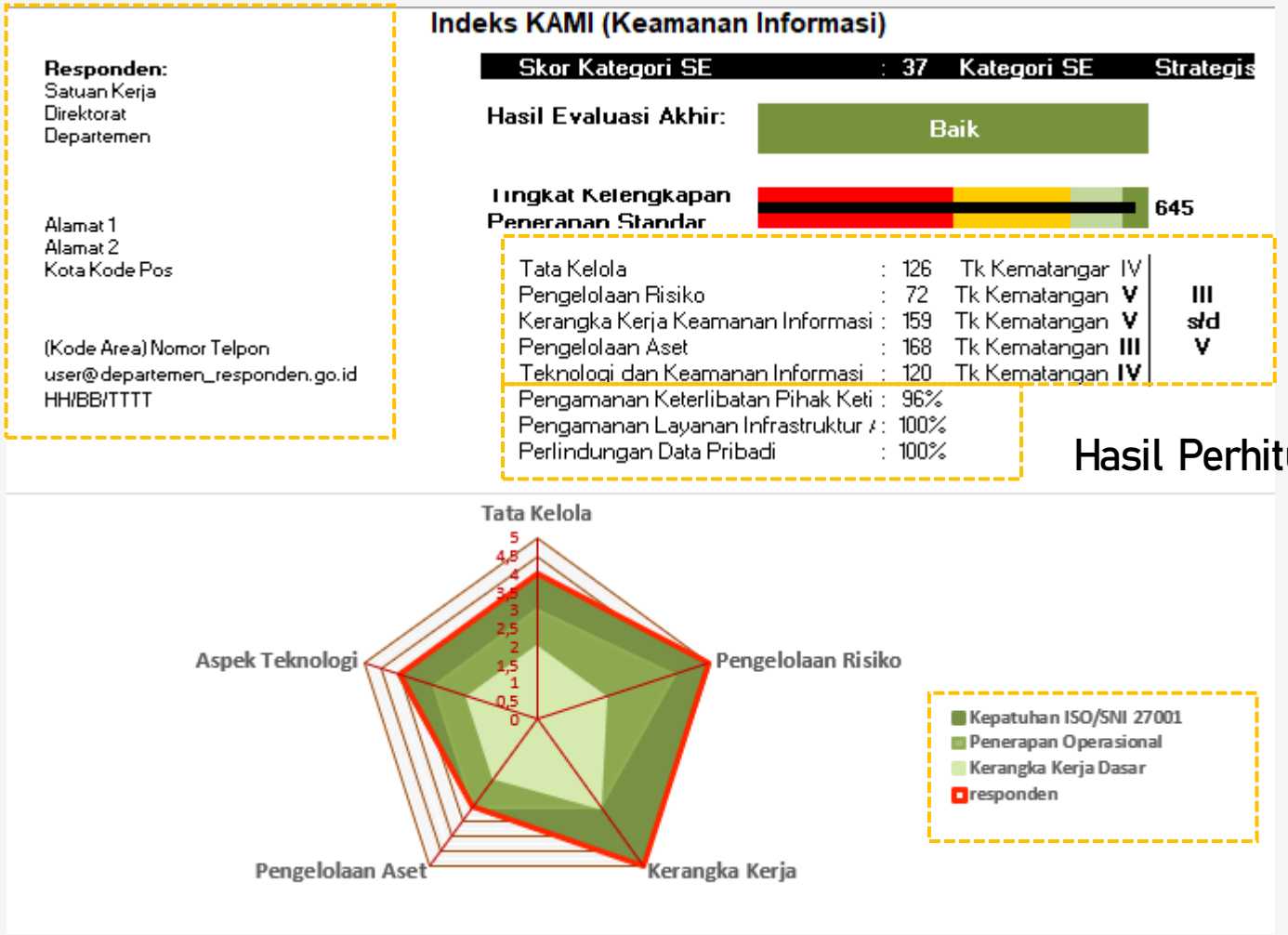


Sesi-2

- Area Indeks KAMI & Praktik Pengisian Instrumen Indeks KAMI v.4.2 rev-3

Dashboard Hasil Penilaian

Identitas Responden



Hasil Perhitungan Tiap Area dan Tingkat Kematangan

Hasil Perhitungan Suplemen

Kepatuhan thd ISO 27001

Instrumen Indeks KAMI versi 4.2 rev-3

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
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Dalam Perencanaan
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?	Diterapkan Secara Menyeluruh
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

Kondisi pada saat memilih jawaban

Pengelompokan Pengamanan sesuai Kategori Kelengkapan

Kategori 1	Kerangka kerja dasar keamanan informasi
Kategori 2	Penilaian tingkat efektivitas dan konsistensi penerapannya
Kategori 3	Kemampuan untuk selalu meningkatkan kinerja keamanan informasi

Pengelompokan Pengamanan sesuai Tingkat Kematangan

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

Keterangan Kondisi Pemilihan Jawaban

Pilihan Jawaban

1 Tidak Dilakukan

- Tidak memiliki dokumen kebijakan dan/ atau prosedur

2 Dalam Perencanaan

- Sudah menjadi rencana resmi instansi dan akan dilaksanakan melalui kegiatan internal/proyek
- Kebijakan/prosedur pengamanan dalam versi konsep (belum resmi)

3 Dalam Penerapan atau Diterapkan Sebagian

- Proyek/kegiatan sedang berjalan atau diterapkan secara bertahap
- Kebijakan/prosedur sudah dirilis secara resmi tetapi asih tahap implementasi

4 Diterapkan Secara Menyeluruh

- Sudah berjalan di seluruh area sesuai dengan ruang lingkup yang didefinisikan

	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

Kategori Sistem Elektronik

10 Butir Kontrol

1

#I. Kategori Sistem Elektronik (1/2)

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

#I. Kategori Sistem Elektronik (2/2)

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] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	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.	

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 dg 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

Kategori SE		Skor Akhir		Status Kesiapan
Rendah				
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi				
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis				
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

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 SE menentukan Hasil Evaluasi Akhir

Hasil Evaluasi Akhir: **Cukup**

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori SE

329

Skor Kategori SE	: 10	Kategori SE		**Rendah**
Tata Kelola	: 48	Tk Kematangan:	II	
Pengelolaan Risiko	: 34	Tk Kematangan:	II	I+
Kerangka Kerja Keamanan Informasi	: 54	Tk Kematangan:	I+	s/d
Pengelolaan Aset	: 123	Tk Kematangan:	II	II
Teknologi dan Keamanan Informasi	: 70	Tk Kematangan:	II	

Hasil Evaluasi Akhir: **Perlu Perbaikan**

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori SE

329

Skor Kategori SE	: 18	Kategori SE		**Tinggi**
Tata Kelola	: 48	Tk Kematangan:	II	
Pengelolaan Risiko	: 34	Tk Kematangan:	II	I+
Kerangka Kerja Keamanan Informasi	: 54	Tk Kematangan:	I+	s/d
Pengelolaan Aset	: 123	Tk Kematangan:	II	II
Teknologi dan Keamanan Informasi	: 70	Tk Kematangan:	II	

Hasil Evaluasi Akhir: **Tidak Layak**

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori SE

329

Skor Kategori SE	: 50	Kategori SE		**Strategis**
Tata Kelola	: 48	Tk Kematangan:	II	
Pengelolaan Risiko	: 34	Tk Kematangan:	II	I+
Kerangka Kerja Keamanan Informasi	: 54	Tk Kematangan:	I+	s/d
Pengelolaan Aset	: 123	Tk Kematangan:	II	II
Teknologi dan Keamanan Informasi	: 70	Tk Kematangan:	II	

Tata Kelola

22 Butir Kontrol

2

Tujuan

Mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas, dan tanggung jawab pengelola keamanan informasi.

Area Evaluasi

Leadership & Komitmen	2.1
Tugas & Tanggung Jawab	2.2-2.5, 2.12-2.14, dan 2.21-2.22
Personil	2.6-2.9
Integrasi Persyaratan Keamanan Informasi	2.10
Pengelolaan Data Pribadi	2.11
Pengelolaan Kinerja	2.15-2.20

#	Kontrol	Eviden
2.1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	- program keamanan informasi yg dilegalisasi pimpinan (Kadis) : Pergub, Perwal, Perbup-> tusi Kadis nya - perkin, SKP, dokumen draf SMKI - dokumen kebijakan keamanan informasi - dokumen rencana strategis
2.2	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	dokumen - uker yg khusus mengelola kam info? tugas tgg jwbnya? : Pergub, Perwal, Perbupttg struktur organisasi dan uraian tugas; SP/SK Tim SMKI.
2.3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkandan menjamin kepatuhanprogram keamanan informasi?	dokumen - sama dgn 2.2: wewenang - SO, RKO, Anjab
2.4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengeloladan menjamin kepatuhanprogram keamanan informasi?	dokumen - dokumen perencanaan program & anggaran yang diajukan pertama kali, terlihat jumlah personil - ABK, Anjab
2.5	Apakah peran pelaksanapengamanan informasi yang mencakup semua keperluan dipetakandengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	dokumen - sama 2.2 & 2.3 : PerGub/Wal/Bup, SP/SK ygterdapat peran -> lebih rinci lagi program/ giatnya - untuk audit internal, siapa yg pegang? peran nya apa? - pengelola aset siapa? pengelola risiko siapa?
2.6	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksanapengelolaan keamanan informasi?	dokumen - sambung 2.7 & 2.9 - standar kompetensi (biasanya di Anjab) - pelaksana pengelolaan kam info siapa? nah standar kompetensi nya apa sbg pelaksana SMKI?
2.7	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	dokumen - standar kompetensi (relasi dg 2.6 & 2.9) - sertifikat pelatihan - sertifikasi keahlian - bisa susun daftar kompetensi personil
2.8	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	dokumen - und, notulen/laporan, dokumentasi : sosialisasi (terkat kaminfo, sec awareness, pengg password) - ss -> infografis di medsos/web, email broadcast praturan, portal pegawai

#	Kontrol	Eviden
2.9	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	dokumen - relasi dg 2.6 & 2.7 - surat pengajuan kegiatan pelatihan (ke bagian kepeg, bappeda, dll) - dokumen rencana program pelatihan
2.10	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerjayang ada?	dokumen - SOA di klausul ISO 27001 - memperbaiki SOP yg ada, penambahan aspek keamanan -> bagian bisnis proses dr organisasi (laporan giat blm jd suatu regulasi, dan blm tentu jd rekomendasi yg ditindaklanjuti)
2.11	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundanganyang berlaku?	dokumen - kebijakan/peraturan identifikasi data pribadi - jika adanya gambaran umum di PerGub/Wal/Bup, dibuatkan turunannya (dokumen SMKI misal) terkait pengelolaan data pribadi ? klasifikasi informasi/data
2.12	Apakah tanggungjawabpengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal daneksternal maupunpihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan(misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	dokumen - relasi dg 2.2 - sudah tertuang di tanggung jwb pengelola kaminfo? - NDA dgn pihak ketiga (NDA ITSA, NDA maintenance jaringan/internet) - perjanjian tenaga kontrak untuk TIK (internal)
2.13	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?	dokumen - relasi dg 2.12 - nota dinas, laporan kegiatan (internal) - laporan urusan persandian (eksternal)
2.14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK(business continuitydan disaster recovery plans) sudah didefinisikan dan dialokasikan?	dokumen - prosedur BCP & DRP (strategi keberlangsungan giat)
2.15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	dokumen - laporan, tinjauan manajemen

#	Kontrol	Eviden
2.16	Apakah kondisi dan permasalahan keamanan informasidi instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	dokumen - relasi dg 2.15 - identifikasi risiko (jika ada) ? identifikasi isu internal dan eksternal terkait kaminfo
2.17	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasiyang menjadi tanggungjawabnya?	dokumen - program khusus di renja, roadmap, SMKI, spesifik di IKU/ Perkin
2.18	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?	dokumen - Perkin, IKU > metode pengukuran pencapaian sasaran - laporan pemantauan/ monitoring evaluasi
2.19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu(pejabat & petugas) pelaksananya?	dokumen - laporan program kegiatan yg tertuang di IKU/ Perkin/ SKP - Perkin dan SKP (individu) - hasil pengukuran kinerja
2.20	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikanuntuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	dokumen - relasi dg2.15 & 2.16 - notulen/ laporan tahunan/ triwulan, tinjauan manajemen, manajemen review - hasil monev
2.21	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnyaterkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	dokumen - daftar induk dokumen (identifikasi seluruh regulasi, kebijakan/peraturan) sampai dengan SOP/ prosedur lebih baik
2.22	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum(pidana dan perdata)?	dokumen - prosedur/ SOP penanganan insiden

PENGELOLAAN RISIKO KEAMANAN INFORMASI

16 Butir Kontrol

3

Tujuan

Mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

Area Evaluasi

Program Kerja	3.1
Penanggung Jawab	3.2
Kerangka Kerja	3.3-3.5, 3.15
Penilaian Risiko	3.6-3.9
Penanggulangan Risiko	3.10-3.13
Perbaikan Berkelanjutan	3.14-3.15

#	Kontrol	Eviden
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Program/ kegiatan keamanan manajemen risiko keamanan informasi
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Unit penanggungjawab manajemen risiko keamanan informasi dan uraian tugas
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Kebijakan/ Prosedur Manajemen Risiko Kaminfo yang mencakup: 1. Metode Penilaian Risiko 2. Kriteria Risiko 3. Proses Penilaian Risiko 4. Risk Owner n Custodian 5. Risk Review terkait Efektifitas
3.4	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?	
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	
3.6	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?	Daftar inventaris aset informasi dan kepemilikannya Risk Register
3.7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Risk Register
3.8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	
3.9	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)?	

#	Kontrol	Eviden
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Risk Treatment Plan
3.11	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?	
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Hasil pemantauan penerapan rencana penanggulangan risiko
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Bukti reviu risk register (Dapat disatukan dalam notulen rapat/ manajemen reviu)
3.14	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?	Bukti reviu (Dapat disatukan dalam notulen rapat/ manajemen reviu)
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Kebijakan/ Prosedur Manajemen Risiko Kaminfo yang mencakup: 1. Metode Penilaian Risiko 2. Kriteria Risiko 3. Proses Penilaian Risiko 4. Risk Owner n Custodian 5. Risk Review terkait Efektifitas
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Bukti reviu (Dapat disatukan dalam notulen rapat/ manajemen reviu)

KERANGKA KERJA KEAMANAN INFORMASI

29 Butir Kontrol

4

Tujuan

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

Area Evaluasi

Kebijakan dan Prosedur	4.1-4.9, 4.19
Pengembangan Sistem	4.10-4.14
Business Continuity Plan & Disaster Recovery Plan	4.15-4.18
Strategi Penerapan Kaminfo	4.20-4.22, 4.27, 4.29
Audit Internal	4.23-4.26, 4.28

#	Kontrol	Eviden
##	Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi	
4.1	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?	Dokumen yang dapat menjelaskan peran dan tanggungjawab semua pihak yang terkait
4.2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Semua dokumen kebijakan, pedoman/panduan dan SOP/Juklak yang sudah dilegalkan Contoh komunikasi yang sudah ada (JDIH, website, media sosial)
4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Daftar Induk Dokumen (didalamnya ada nomor, revisi/versi, status distribusi, status Rilis/Draft)
4.4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Jadwal dan sasaran kebijakan serta komunikasi yang digunakan (dapat melalui proses pelaksanaan Pelatihan, Sosialisasi , Diseminasi)
4.5	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?	Kebijakan dan prosedur yang disusun untuk meminimalisir risiko hasil identifikasi risk assessment (Dok Risk Register) atau untuk memenuhi sasaran tertentu
4.6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Kebijakan/Prosedur tentang identifikasi event dan bagaimana ditetapkan sebagai insiden, kemudian penyelesaian / recover, misal melalui Risk Value dan Treatment pada Risk Register
4.7	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?	Kontrak dengan Pihak Ketiga yang harus terdapat kewajiban Laporan Insiden, Service Level Agreement (SLA) hingga maintenance
4.8	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	kebijakan atau aturan kepegawaian, atau NDA didalamnya terdapat aspek keamanan dan sanksi
4.9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?	Kebijakan yang mengatur adanya pengecualian dan siapa yang dapat menyetujuinya
4.10	Apakah organisasi 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?	SOP patch dan SK Penanggung Jawab

#	Kontrol	Eviden
##	Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi	
4.11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Pengaturan hak akses, pengamanan data penting, NDA, monitoring keamanan infrastruktur, jaringan server, SOP manajemen kerentanan
4.12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dokumen Evaluasi Rencana Pengadaan/Implementasi Sistem TI Dokumen Monitoring dan Evaluasi Risiko
4.13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	SOP pengembangan sistem hingga sampai penerapannya tentang Secure SDLC
4.14	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?	Dokumen Risiko berikut penerapan dan bukti-buktinya
4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	kebijakan, prosedur, rencana implementasi misal seklai tiap tahun dalam bulan mei
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	SK Tim yang bertanggungjawab dan masing-masing perannya
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?	Kebijakan Penjadwalan BCP
4.18	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?	Kebijakan BCP dalam hal evaluasi dan perbaikan
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Daftar Induk Dokumen, Berita Acara, Notula Rapat Evaluasi

#	Kontrol	Eviden
##	Pengelolaan Strategi dan Program Keamanan Informasi	
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Risk Register menggambarkan mitigasi risiko, Apakah KPI/IKU, RKA, DPA menggambarkan kebutuhan mitigasi risiko dan keinginan penyempurnaan/Perbaikan proses SMKI
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Misal dokumen KAK Pembelian Software/ Sistem
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Bukti Implementasi pada nomor 20 dan 21 serta alokasi tersedianya anggaran untuk Penerapan Keamanan Informasi (aktualisasi program kerja)
4.23	Apakah organisasi 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)?	SK Audit Internal dalam Keamanan Informasi
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	SOP Audit, Audit Plan, Laporan Audit, Tindak Lanjut Audit, laporan monitoring Tindak lanjut
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Audit Plan, Laporan Audit, TindakLanjut Audit, laporan monitoring Tindak lanjut
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Audit Plan, Laporan Audit, TindakLanjut Audit, laporan monitoring Tindak lanjut
4.27	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?	Manajemen review dan MoM nya
4.28	Apakah organisasi 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?	Terhadap pelaksanaan Monev Penerapan/Kepatuhan
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Road Map, Cascading, RKA sesuai dengan Roadmap. dan perubahan yang terdokumentasi. Renstra, Renja, RPJMD.

PENGELOLAAN ASET

36 Butir Kontrol

5

Tujuan

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

Area Evaluasi

Aset Informasi	5.1-5.7
Kontrol Keamanan Penerapan Mitigasi Risiko	5.8-5.27
Pengamanan Akses	5.28-5.29, 5.37-5.38
Pengamanan Aset Fisik dan Gedung	5.30-5.36

#	Kontrol	Eviden
##	Pengelolaan Aset Informasi	
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)	Aset Register/ Inventaris Aset dengan pemilik aset.
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	- Kebijakan/Prosedur Klasifikasi Aset Informasi dan Pengamanannya
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	- Kebijakan/Prosedur Pengelolaan Hak Akses - Periksa matriks user akses. Bisa dalam bentuk akses kontrol
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	- Kebijakan/Prosedur Change Management - Laporan perubahan sistem, proses TI, konfigurasi maupun proses bisnis - Ada SOP manajemen perubahan dan bukti implementasinya?
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	- Kebijakan/Prosedur Pengelolaan Konfigurasi Akses konfigurasi system TI dibatasi? Konfigurasi di backup?
5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	- Kebijakan/Prosedur Change Management - Ada SOP change management dengan cakupan sampai rilis? SOP Change Mgm dapat dipisah atau disatukan dengan SOP Relase Mgm.

#	Kontrol	Eviden
##	Pengelolaan Aset Informasi	
###	Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
5.8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Dokumen kontrak kerja
5.9	Tata tertib penggunaan komputer, email, internet dan intranet	Kebijakan/ketentuan penggunaan Komputer, email, Internet, social media, dsb
5.10	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	- Kebijakan/Prosedur Penggunaan Aset dalam pengelolaan informasi
5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	- Kebijakan/Prosedur Instalasi Software dan Penggunaan lisensi
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Prosedur/SOP penggunaan data pribadi
5.13	Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya	- Kebijakan Manajemen Password
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	- Kebijakan/Prosedur Penggunaan Aset dalam pengelolaan informasi
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	- Kebijakan/Prosedur Retensi Informasi Berklasifikasi Penghancuran Informasi dan Media Penyimpanan Informasi yang tidak digunakan - Ada SOP handling & Disposal Informasi?
5.16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	NDA yang berisikan proses pertukaran data dijamin akan menjaga informasi yang diberikan
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Digital Forensik bagian dari ini. Berkaitan dengan aspek Hukum, untuk pelanggaran2 yang memiliki dampak hukum. - Laporan Investigasi Insiden Keamanan Informasi
5.18	Prosedur back-up dan uji coba pengembalian data (restore) secara berkala	- Kebijakan/Prosedur Back Up dan Restore - SOP Backup Restore dan buktinya - Laporan back up dan restore berkala
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	- Kebijakan/Prosedur Pengamanan Fisik Apa saja ruangan yang ditetapkan kritikal, apa kontrolnya Misal untuk DC akses dibatasi, diawasi CCTV, Genset

#	Kontrol	Eviden
##	Pengelolaan Aset Informasi	
###	Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
5.20	Proses pengecekan latar belakang SDM	- Kebijakan/Prosedur Manajemen SDM terkait risiko keamanan informasi - Form Ceklist bahwa pengecekan sudah dilakukan
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Jika pelanggaran hukum dilaporkan polisi, Jika misal terkait kebakaran -> damkar. Evidence daftar aduan terupdate
5.22	Prosedur penghancuran data/aset yang sudah tidak diperlukan	- Kebijakan/Prosedur Retensi Infromasi Berklasifikasi Penghancuran Informasi dan Media Penyimpanan Informasi yang tidak digunakan
5.23	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	- Kebijakan/Prosedur Review Hak Akses (User Access Review)
5.24	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.	Periksa SOP dan penerapannya - Kebijakan/Prosedur pengembalian aset saat penghentian kepegawaian, kontrak atau perjanjian
5.25	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?	- Kebijakan/Prosedur Back Up
5.26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Periksa daftar bukti penerapan keamanan: Laporan, Formulir yang sdh diisi, dsb
5.27	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?	- Kebijakan/Prosedur Penggunaan Aset Pihak Ketiga dalam pengelolaan informasi

#	Kontrol	Eviden
#	Pengamanan Fisik	
5.28	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?	- Kebijakan/Prosedur Pengamanan Fasilitas Fisik - Kebijakan/Prosedur Pengamanan Ruang Server, Arsip dan Lokasi Penting Lainnya
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	- Kebijakan/Prosedur Pengamanan Ruang Server, Arsip dan Lokasi Penting Lainnya
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	- Kebijakan/Prosedur Pengamanan Ruang Server, Arsip dan Lokasi Penting Lainnya - Laporan Pemantauan suhu, kelembaban, hasil pengukuran grounding system
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	- foto, SOP, POK -> perawatan, genset - Kebijakan/Prosedur Pengamanan Ruang Server, Arsip dan Lokasi Penting Lainnya
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Kebijakan/Prosedur pengamanan perangkat
5.33	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)?	- Formulir keluar masuk barang/perangkat
5.34	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?	- Kebijakan/Prosedur Pengamanan Ruang Server, Arsip dan Lokasi Penting Lainnya
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	- Laporan Perawatan fasilitas pendukung utama (A/C, Fire estinguisher, alarm, Genset, UPS, grounding system, CCTV, dsb)
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	berita acara serah terima brang. Form surat jalan kurir - Formulir keluar masuk barang/perangkat
5.37	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)	foto larangan - Kebijakan/Prosedur Pengamanan Ruang Server, Arsip dan Lokasi Penting Lainnya
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	- Laporan/Form Pencatatan tamu ruang server, arsip dan ruang penting lainnya

TEKNOLOGI DAN KEAMANAN INFORMASI

26 Butir Kontrol

6

Tujuan

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

Area Evaluasi

Pengamanan Jaringan	6.1-6.4, 6.6-6.7, 6.17-6.18
Pengamanan Sistem	6.5, 6.8-6.10, 6.15-6.16, 6.19-6.26

#	Kontrol	Eviden
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Arsitektur/ Topologi infrastruktur
6.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Topologi jaringan, segementasi jaringan
6.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan,sistem dan aplikasi yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Dokumen konfigurasi standar sistem, jaringan & aplikasi
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Laporan kepatuhan atas Dokumen konfigurasi standar sistem, jaringan & aplikasi
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubaan/keutuhan konfigurasi?	Laporan vulnerability assessment (VA), pentest baik sistem, jaringan & aplikasi
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Kebijakan penerapan redundansi sistem, ketersediaan storage & balance dengan loadnya
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	-Prosedur pemantauan sumberdaya TIK -Monitoring (capture dashboard) : storage, bandwith, utilisasi CPU
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Capture file log
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Capture file log
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Laporan analisis log
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	-Penerapan SSL -enkripsi database
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Kebijakan penggunaan enkripsi (bisa masuk ke dalam standar konfigurasi)
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan , termasuk siklus penggunaannya?	SOP pengelolaan sertifikat elektronik

#	Kontrol	Eviden
6.14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menonaktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?	-SOP penggunaan password -cek langsung pada SE
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	-Prosedur hak akses -Penerapan pengamanan pada akses administrasi sistem: password, pemisahan hak akses
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses?	-Capture session time out, lockout setelah gagal login -Kebijakan/pengaturan dalam penarikan akses
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Catatan log (AP, IDS/IPS, dll)
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	-Capture tools yang digunakan : anti spam, antimalware, password, firewall -Penggunaan teknologi untuk pengamanan Gedung : fingerprint
6.19	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	Capture update pada desktop & server : operating system, antivirus, antimalware
6.20	Apakah setiap dekstop dan server dilindungi dari penyerangan virus (malware)?	-Capture antivirus/antimalware yang digunakan -Laporan monitoring
6.21	Apakah ada rekaman dan hasil analisa (jejak audit) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	-Capture antivirus/antimalware yang telah update -Laporan monitoring
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	-Capture hasil scan antivirus/antimalware yang telah berjalan -Laporan monitoring
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Penerapan pengaturan waktu pada jaringan, sistem & aplikasi (capture NTP)
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan ujicoba?	Dokumen laporan hasil User Acceptance Test (UAT)
6.25	Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan ujicoba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	-Dokumen perencanaan pembangunan aplikasi SSDLC -Laporan penerapan pengamanan pada lingkungan pengembangan dan ujicoba
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	-Hasil pentest/ IT security assessment -Sertifikasi ISO

SUPLEMEN

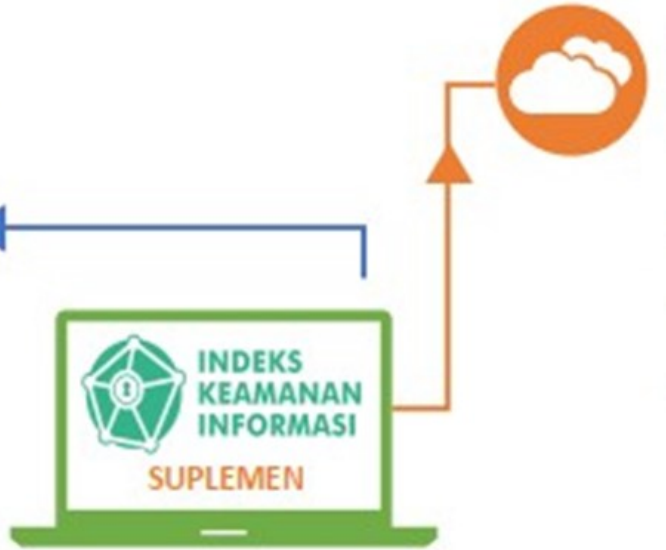
Pihak Ketiga, Cloud Services, PDP

7

Komponen Suplemen

Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan

- Manajemen Risiko dan Pengelolaan Keamanan Pihak Ketiga
- Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga
- Pengelolaan Layanan dan Keamanan Pihak Ketiga
- Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga
- Penanganan Aset
- Pengelolaan insiden oleh Pihak Ketiga
- Rencana Kelangsungan Layanan Pihak Ketiga



Pengamanan Layanan Infrastruktur Awan (Cloud Services)

- Identifikasi (Kajian Risiko, Penyimpanan Data)
- Proteksi (Penerapan Keamanan dan Aspek Regulasi)
- Penanggulangan dan Pemulihan (Gangguan & Insiden)
- Pemantauan dan Pengendalian (Penghentian Layanan)

Perlindungan Data Pribadi

- Kebijakan dan peraturan yang berlaku
- Penyimpanan/dokumentasi Data Pribadi
- Penyimpanan dan Pengiriman Data
- Pemusnahan dan Penghapusan Data
- Pemisahan Tugas dan pihak berkorelasi lainnya
- Tujuan pemanfaatan data, akuntabilatan dan akurasi

#	Kontrol	Eviden
7.1	Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	
7.1.1	Manajemen Risiko dan Pengelolaan Keamanan Pihak Ketiga	
7.1.1.1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Dokumen Risk Register
7.1.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Laporan Penilaian Risiko
7.1.1.3	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Monitoring/ review pelaksaan mitigasi risiko
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Lapaoran Monitoring/ review pelaksaan mitigasi risiko
7.1.1.5	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?	Dokumen NDA
7.1.1.6	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Dokumen Kontrak, NDA
7.1.1.7	Apakah hak audit TI secara berkala ke 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?	Laporan Audit IT Pihak Ketiga
7.1.2	Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga	
7.1.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	Laporan Penilaian Risiko
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Dokumen Kontrak, NDA
7.1.2.3	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	Monitoring/ review pelaksaan subkontraktor

#	Kontrol	Eviden
7.1	Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	
7.1.3	Pengelolaan Layanan dan Keamanan Pihak Ketiga	
7.1.3.1	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?	SOP Pengendalian Akses Pihak Ketiga
7.1.3.2	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	Unit terkait Keamanan Informasi (SK)
7.1.3.3	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	Dokumen Kontrak
7.1.3.4	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	Monitoring/ review pelaksaan Kontrak
7.1.3.5	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?	Risalah Rapat Evaluasi
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	Laporan Audit
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	Laporan Tindaklanjut Audit
7.1.3.8	Apakah kondisi terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	Laporan Tindaklanjut Evaluasi
7.1.4	Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga	
7.1.4.1	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?	Dokumen Adendum Kontrak
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	Monitoring/ review pelaksaan mitigasi risiko

#	Kontrol	Eviden
7.1	Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan	
7.1.5	Penanganan Aset	
7.1.5.1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan/penghancuran aset?	SOP Pengendalian Aset
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	BA Penghancuran/Penghapusan
7.1.6	Pengelolaan Insiden oleh Pihak Ketiga	
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	SOP Penanganan Insiden
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	Dokumentasi / Laporan Penanganan Insiden
7.1.7	Rencana Kelangsungan Layanan Pihak Ketiga	
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	Kebijakan BCP
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	Laporan Pengujian/Drill Test
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	Unit Khusus, SK Tim

#	Kontrol	Eviden
7.2	Pengamanan Layanan Infrastruktur Awan (Cloud Service)	
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	Laporan Penilaian Risiko
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?	Kebijakan mengenai layanan berbasis cloud
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud?	Bukti penerapan pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud
7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?	Kebijakan mengenai layanan berbasis cloud
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?	Dokumen hasil tinjauan penyelenggara (penyedia) layanan cloud
7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	Dokumen Standar keamanan teknis penggunaan layanan cloud
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	Sertifikat
7.2.8	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	Dokumen BCP atau DRP terkait layanan cloud
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	Prosedur pelaporan insiden terkait layanan cloud
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	Prosedur / SOP Pengelolaan Data

#	Kontrol	Eviden
7.3	Perlindungan Data Pribadi	
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	Daftar jenis dan bentuk data pribadi yang disimpan diolah dan dipertukarkan
7.3.2	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	Prosedur / SOP Pengelolaan Data
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	Dokumen Prosedur mengenai mekanisme pengelolaan (pemrosesan, pertukaran dan penyimpanan) data pribadi
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Kebijakan mengenai Perlindungan Data Pribadi
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (Data Protection Officer, Data Controller, Data Processor) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	Surat Perintah DPO, Surat Keterangan Data Controler dan Data Processor
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	Risk Register
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	Dokumen Analisa Risiko terkait dampak kebocoran data pribadi
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	Laporan audit internal
7.3.9	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	Dokumen program kerja instansi
7.3.10	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 ?	Log atau Pernyataan Persetujuan terkait Data Pribadi
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	Prosedur Pelaporan Insiden terkait Data Pribadi
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	Prosedur pengendalian akses Data Pribadi

#	Kontrol	Eviden
7.3	Perlindungan Data Pribadi	
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	Prosedur pemutakhiran Data Pribadi
7.3.14	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	Prosedur periode penyimpanan dan penghapusan data pribadi
7.3.15	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?	SOP Penghapusan Data
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	Prosedur Pengungkapan Data Pribadi untuk keperluan hukum

Terima Kasih