Indeks KAMI

Pelatihan Indeks KAMI

Virtual, 21-22 Juli 2021

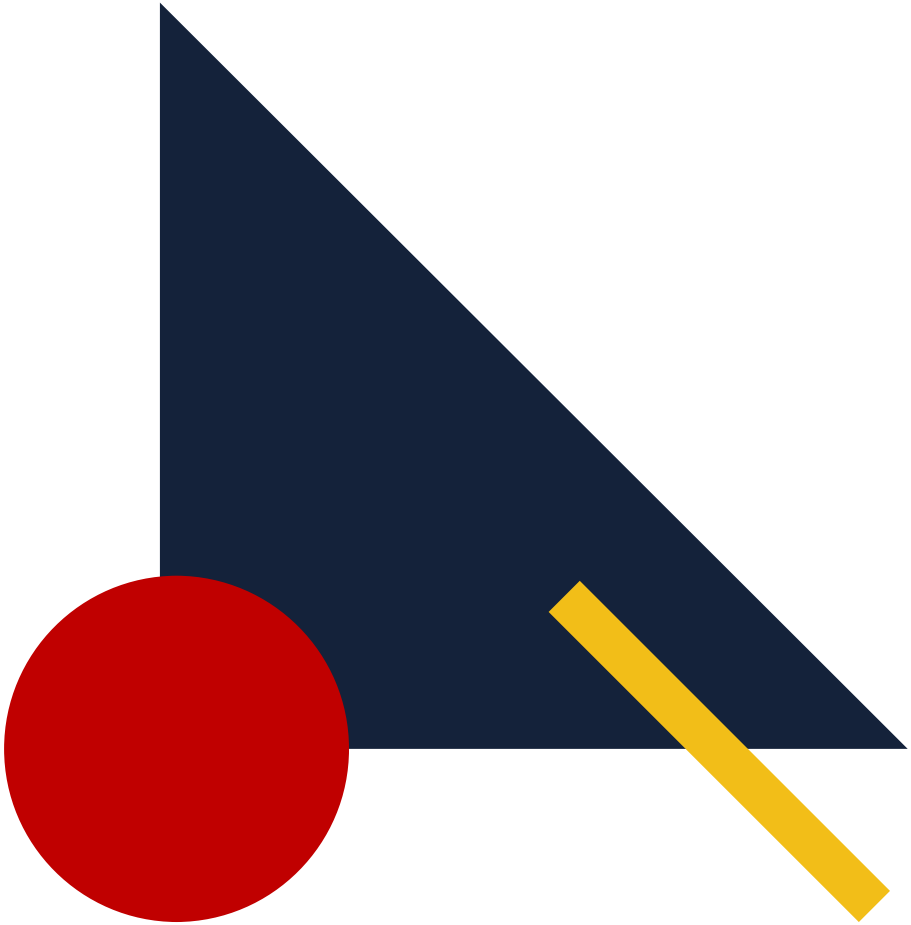
Fasilitator:

- Vira Septiyana Kasma

PROFESIONAL INTEGRITAS ADAPTABILITAS TEKNOLOGI TEPERCAYA

Pelatihan Indeks KAMI

PENGENALAN INDEKS KAMI



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Definisi

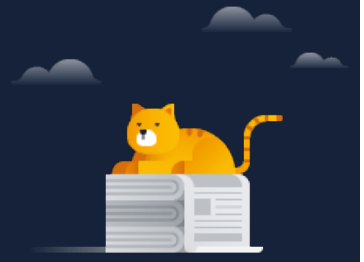
evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di organisasi.

Perban SMPI 8/2020 Pasal 1 Angka 13

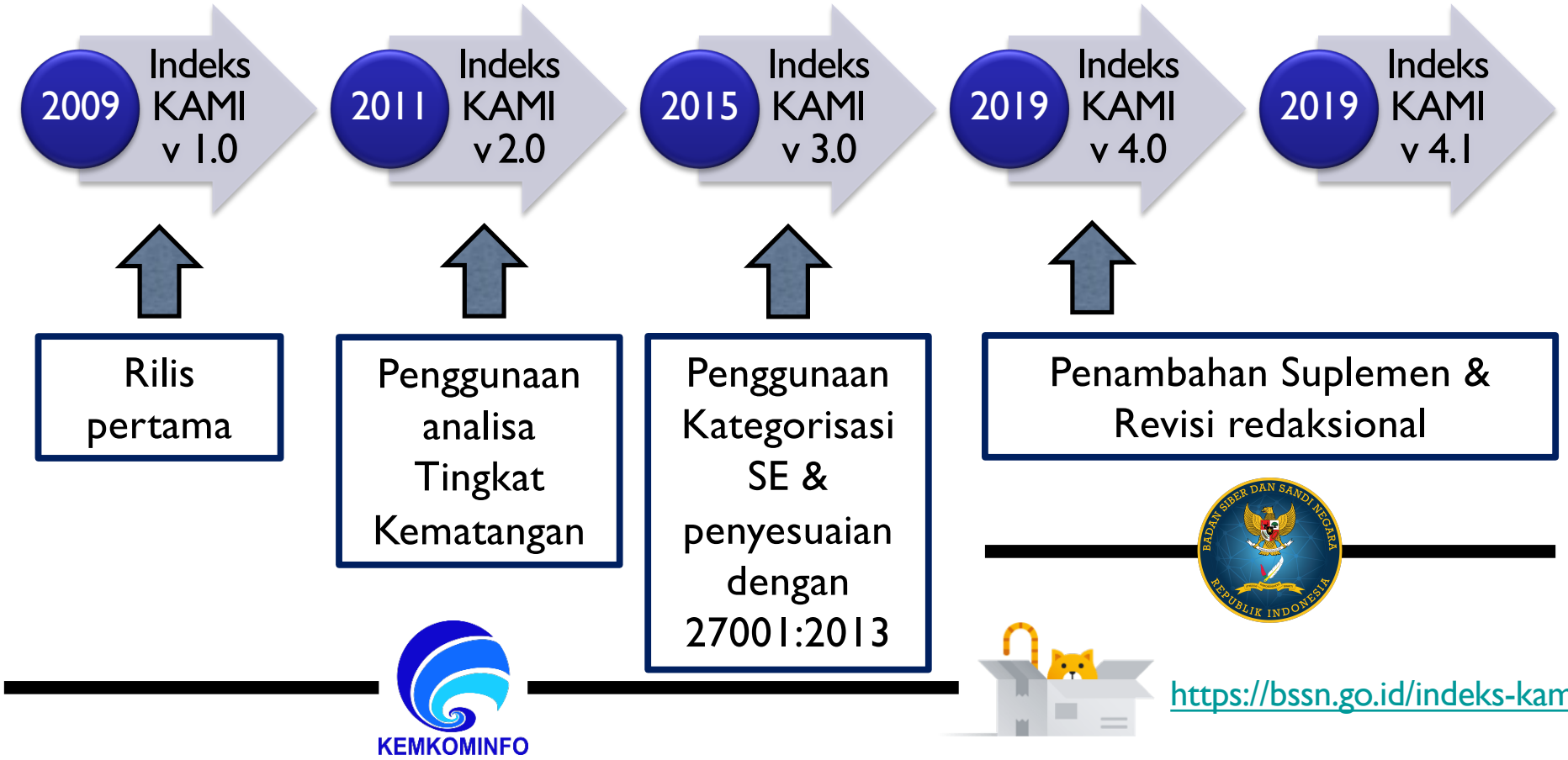
Tujuan

untuk mempersiapkan penerapan SNI ISO/IEC 27001

Perban SMPI 8/2020 Pasal 12 ayat (1)



Evolusi Indeks KAMI



Penilaian Indeks KAMI

BAGIAN

Kategorisasi Sistem Elektronik

Max Tk. II SE rendah = 312
Max Tk. II SE tinggi = 455
Max Tk. II SE strategis = 535

- Tata kelola
- Manajemen Risiko
- Kerangka Kerja
- Manajemen Aset
- Teknologi dan Keamanan Informasi

- Keamanan Pihak Ketiga
- Kemanaan Layanan Cloud
- Pelindungan Data Pribadi

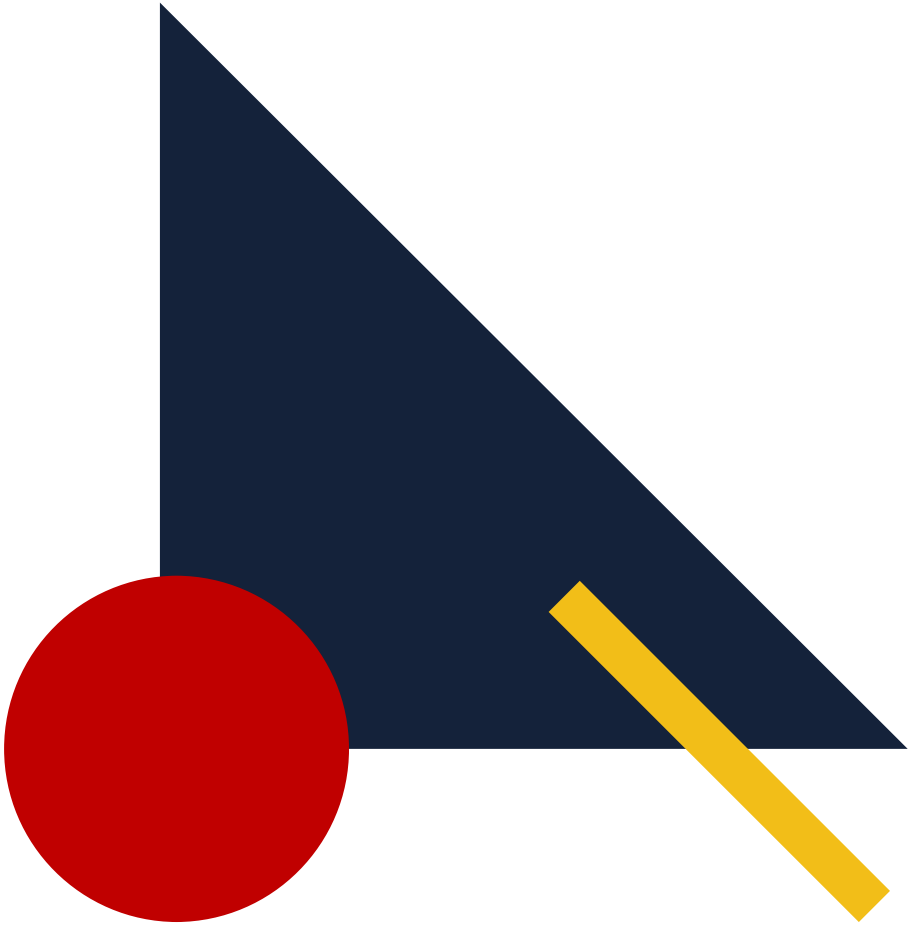
Persentase penerapan

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

Pelatihan Indeks KAMI

KATEGORI SISTEM ELEKTRONIK



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Lingkup

(Identitas Responden)

Identitas Instansi atau Perusahaan	Satuan Kerja Direktorat Departemen
Alamat	Alamat 1 Alamat 2 Kota Kode Pos
Nomor Telpon	(Kode Area) Nomor Telpon
Email	user@departemen_responden.go.id
Pengisi Lembar Evaluasi	Nama Staf atau Pejabat
Jabatan	Jabatan Struktural/Fungsional
Tanggal Pengisian	HH/BB/TTTT
Deskripsi Ruang Lingkup	
Isi dengan deskripsi ruang lingkup struktur organisasi (Departemen, Bagian atau Satuan Kerja) dan infrastruktur TIK	

Kriteria Kategorisasi*

Karakteristik SE	A = 5	B = 2	C = 1
1. Nilai Investasi	A > 30 M	3M < B < 30 M	C < 3 M
2. Total anggaran Operasional Tahunan	A > 10 M	1M < B < 10 M	C < 1 M
3. Kewajiban peraturan atau standar tertentu	Peraturan atau Standar Nasional + Internasional	Peraturan atau Standar Nasional	Tidak ada
4. Penggunaan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik	Teknik kriptografi khusus yang disertifikasi oleh Negara	Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri	Tidak ada penggunaan Teknik kriptografi
5. Jumlah Pemilik Akun	A > 5.000	1.000 < B < 5.000	C < 1.000
6. Pengelolaan Data Pribadi (DP)	DP memiliki hubungan dengan DP lainnya	DP individu, yang berkaitan dengan kepemilikan Badan Usaha	Tidak ada DP
7. Klasifikasi Kekritisan Data	Sangat Rahasia	Rahasia / terbatas	Biasa
8. Tingkat Kekritisan Proses	Berdampak langsung pada layanan publik	Berdampak tidak langsung pada layanan publik	Tidak berdampak
9. Dampak Kegagalan	Layanan publik skala nasional atau membahayakan pertahanan negara	Layanan publik skala provinsi atau lebih	Skala Kabupaten/Kota atau lebih
10. Potensi Kerugian atau dampak negatif Insiden	Menimbulkan korban jiwa	Kerugian Finansial	Gangguan operasional sementara

*Sesuai Perban BSSN SMPI 8/2020

Pengaturan dalam Kategorisasi

NO	KARAKTERISTIK SISTEM ELEKTRONIK	BOBOT NILAI		
		A = 5	B = 2	C = 1
Total Bobot Nilai	:			
KETENTUAN PENILAIAN				
Kategori Sistem Elektronik		STRATEGIS	TINGGI	RENDAH
Total Bobot nilai		36–50	16–35	≤ 15

a. SNI ISO/IEC 27001; **dan**
b. standar keamanan lain yang ditetapkan oleh BSSN; **dan**
c. standar keamanan lain yang tetapkan oleh K/L Sektor

a. SNI ISO/IEC 27001 **dan/atau** standar keamanan lain yang ditetapkan oleh BSSN; **dan**
b. standar keamanan lain yang tetapkan oleh K/L Sektor

a. SNI ISO/IEC 27001; **atau**
b. standar keamanan lain yang ditetapkan oleh BSSN

Pelatihan Indeks KAMI

ASPEK TATA KELOLA

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Pendahuluan

(Penilaian & Status Penerapan)

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

Pengelompokan Pengamanan sesuai Kategori Kelengkapan

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

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

AREA YANG DIEVALUASI

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

1. ***Leadership* dan komitmen** (2.1)
2. **Tugas dan tanggung jawab** (2.2 – 2.4), (2.12 – 2.14), dan (2.21 – 2.22)
3. **Personil** (2.6 – 2.9)
4. **Integrasi Persyaratan Keamanan Informasi** (2.10)
5. **Pengelolaan Data Pribadi** (2.11)
6. **Pengelolaan Kinerja** (2.15 – 2.20)

DOKUMEN YANG DIBUTUHKAN

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)
- ✓ Prosedur BCP/ DRP beserta tim penanggung jawab (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)

DOKUMEN YANG DIBUTUHKAN

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 diska lepas 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)

DOKUMEN YANG DIBUTUHKAN

Implementasi berupa:

- ✓ 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 surat menyurat (2.12 – 2.13)
- ✓ Laporan berkala implementasi/ progres SMKI dan monev, termasuk tindak lanjut audit, penanganan risiko, pada pimpinan (2.15 – 2.20)
- ✓ Hasil pengukuran kinerja SMKI/ progres capaian (2.15 – 2.20)
- ✓ Daftar undang-undang, regulasi, peraturan, standar keamanan informasi yang harus dipatuhi (2.21)

Pelatihan Indeks KAMI

ASPEK MANAJEMEN RISIKO

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

AREA YANG DIEVALUASI

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

1. **Program kerja pengelolaan risiko** (3.1)
2. **Penanggung jawab pengelolaan risiko** (3.2)
3. **Kerangka kerja pengelolaan risiko** (3.3 – 3.5) dan (3.15)
4. **Penilaian Risiko** (3.6 – 3.9)
5. **Penanggulangan Risiko** (3.10 – 3.13)
6. **Perbaikan berkelanjutan** (3.14 – 3. 16)

DOKUMEN YANG DIBUTUHKAN

Kebijakan keamanan informasi (2.1), yang di dalamnya terdapat **kebijakan/ prosedur** Manajemen Risiko Kaminfo yang mencakup (3.2 – 3.5)*:

1. metode penilaian risiko
2. kriteria risiko
3. proses penilaian risiko
4. pembagian peran seperti unit penanggung jawab, risk owner dan custodian serta tugas, wewenang dan tanggung jawabnya
5. mekanisme eskalasi risiko sampai tingkat pimpinan
6. mekanisme risk review terkait efektifitas (3.15)

* Dapat digabung atau dipisah dari kebijakan keamanan informasi pada area II

DOKUMEN YANG DIBUTUHKAN

- ✓ **Program**/ kegiatan manajemen risiko keamanan informasi (3.1)

Implementasi pengelolaan risiko melalui:

- ✓ Daftar inventaris aset informasi dan kepemilikannya Risk Register (3.6)
- ✓ *Risk Register* (3.7 – 3.9)
- ✓ *Risk Treatment Plan* (3.10 – 3.11)
- ✓ Hasil pemantauan penerapan rencana penanggulangan risiko (3.12 – 3.13)
- ✓ Bukti reviu pengelolaan risiko termasuk *risk register*, profil risiko, mitigasi dan kerangka kerja pengelolaan risiko (dapat dibuat bersamaan dalam notulen rapat/ manajemen reviu) (3.12 – 3.15)
- ✓ Bukti *Risk Treatment* telah berhasil melakukan mitigasi risiko (3.16)

TERIMA KASIH

Amankan Informasi Anda!!!

PROFESIONAL INTEGRITAS ADAPTABILITAS TEKNOLOGI TEPERCAYA