INDEKS KAMI (Keamanan Informasi)

Assoc.Prof. Dr. Muhammad Said Hasibuan,S.Kom.,M.Kom
Fakultas Ilmu Komputer IIB Darmajaya
2025

Definisi

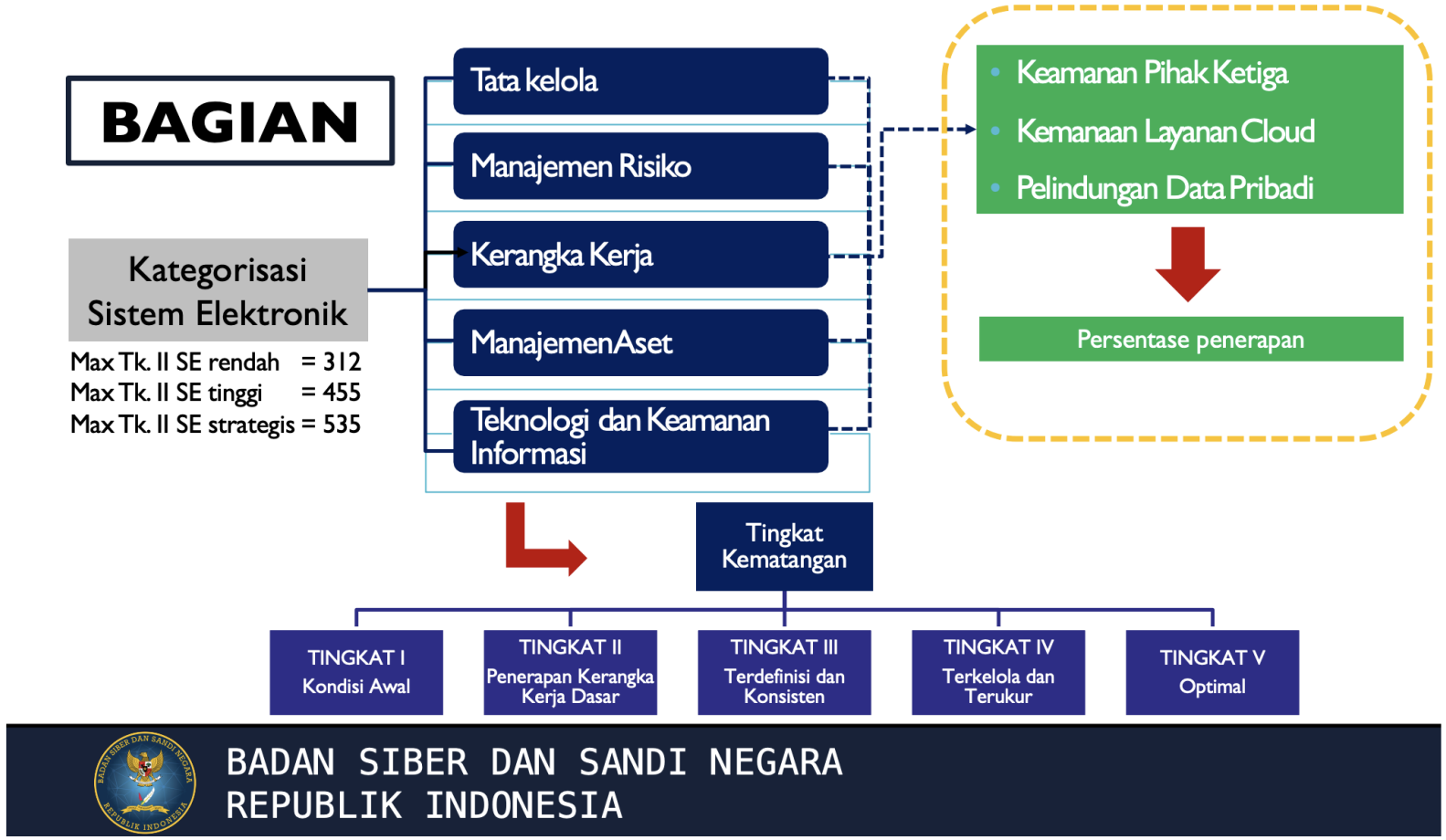
- Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi.
- Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan.

Definisi

- 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 27001:2013.
- Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah

Evolusi Indeks KAMI

Penilaian Indeks KAMI



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

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

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

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

Kategori I	Kerangka kerja dasar keamanan informasi
Kategori 2	Penilaian tingkat efektifitas 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

AREA YANG DIEVALUASI

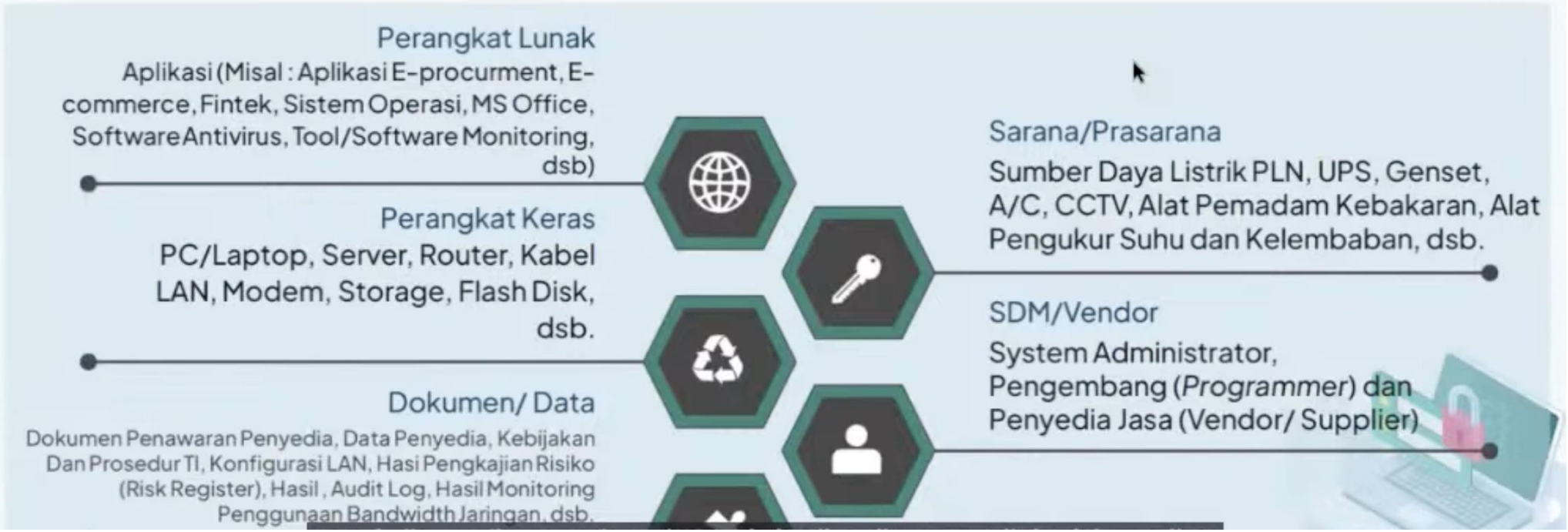
Mengevaluasi kesiapan bentuk tata kelola pengamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi

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)

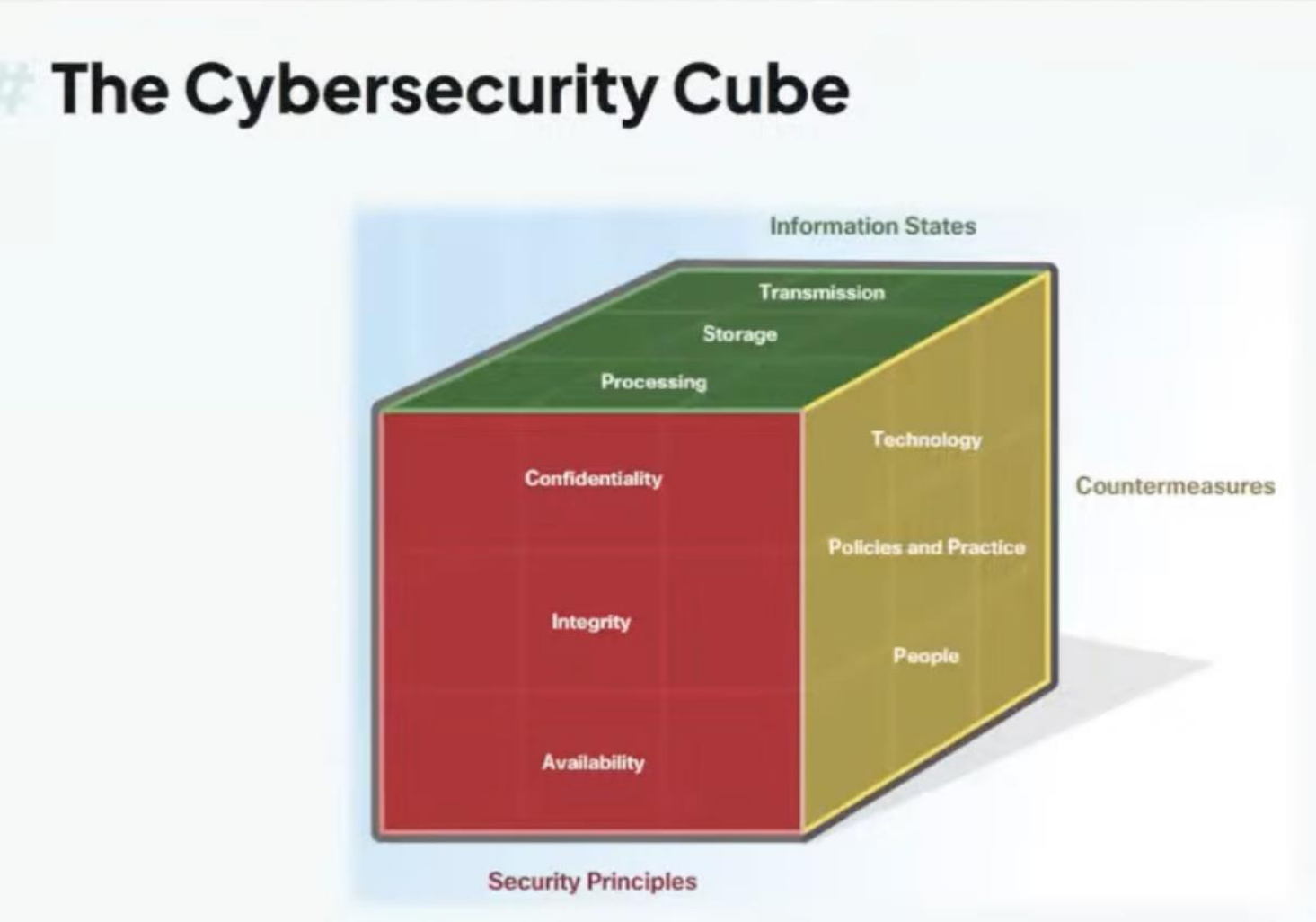
BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Aset Informasi

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



In 1991, John Mc Cumbers created a comprehensive security model called **McCumbers cube** or the **CyberSecurity Cube**.



First Dimension Security Principles

C: Confidentiality

- *Authentication* (verifies the identity of a user to prevent unauthorized access);
- *Authorization (*services determine which resources users can access, along with the operations that users can perform);
- *Accounting (*keeps track of what users do, including what they access, the amount of time they access resources, and any changes made)

I : Integrity

Another term for integrity is **quality**. Integrity is about maintaining the consistency, accuracy, and trustworthiness of information over its entire life cycle. Protecting the integrity of data is challenging, loss of data integrity can make entire data resources unreliable and unusable.

- Methods used to ensure data integrity including data consistency checks, access control, hashing, data validation

A: Availability

Assures that a system's authorized users have timely and uninterrupted access to the information in the system and the network.

- We can ensure availability by following these activities such as a plan for disasters, test backups, equipment maintenance, monitor unusual activity.

Second Dimension Information States

A. Processing

- Data in process refers to data during initial input, modification, compilation, or output.

B. Storage (Stored data)

- Stored data often refers to Data at rest. Data at rest means that a type of storage device retains the data when no user or process is using it.

C. Transmission

- Transmission involves sending information from one device to another. The challenges in this process are: protecting data confidentiality, protecting data integrity, protecting data availability

Third Dimension
Counter measurement

a. Technologies

- Some technology that can be used to safe us from cyber-attacks are Content Filtering, Firewall Appliances, Virtual Private Network (VPN), Network Access Control (NAC), etc.

b. Education, training, and awareness.

- Technologies tools are not enough to defeat cyber criminals. The user also needs to follow good practices to stay safe.

c. Policies and Procedures

- Good policies, procedures, and guidelines are needed to enable users to stay safe in cyberspace. ISO published ISO 27000, even though it's not mandatory but most countries use ISO 27000 as a de facto framework for implementing their information security management.

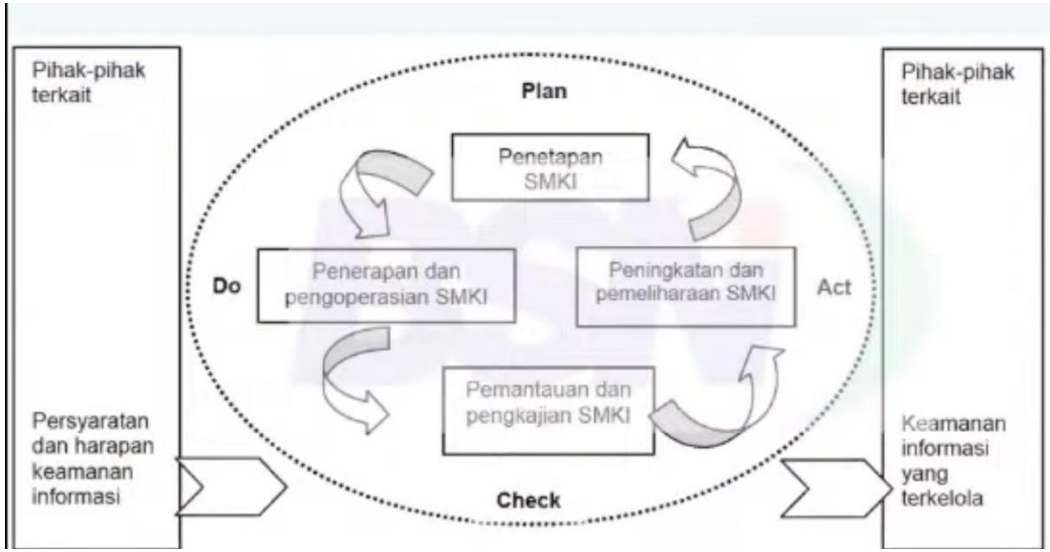
SMKI merupakan suatu proses yang disusun berdasarkan pendekatan berbasis risiko untuk merencanakan (Plan), mengimplementasikan dan mengoperasikan (Do), memonitor dan meninjau ulang (Check) serta memelihara dan meningkatkan (Act) keamanan informasi organisasi.

(SNI ISO/IEC 27001:2022)

Dasar Hukum SMKI

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

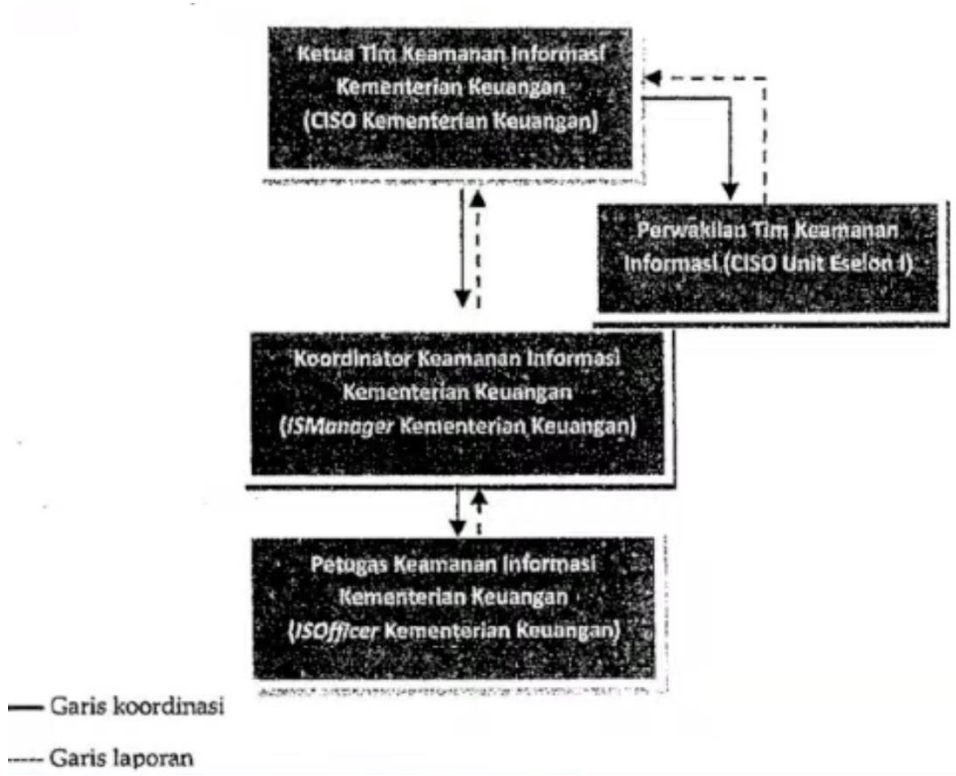
Model PDCI

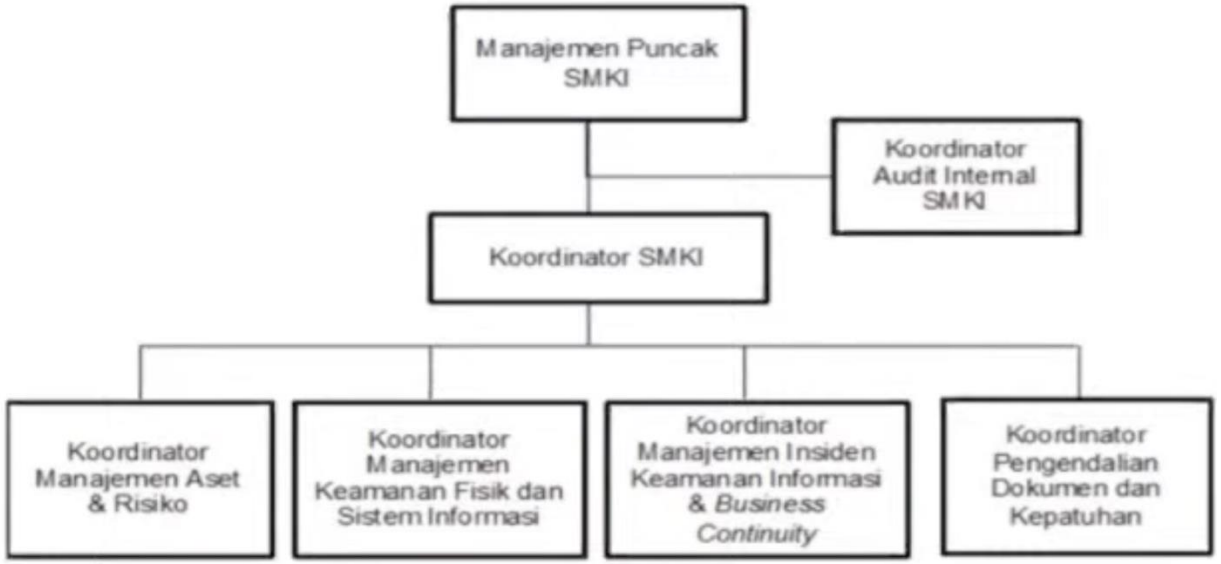


***Plan* (penetapan SMKI)**	Menetapkan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.
***Do* (penerapan dan pengoperasian SMKI)**	Menerapkan dan mengoperasikan kebijakan, pengendalian, proses dan prosedur SMKI.
***Check* (pemantauan dan pengkajian SMKI)**	mengases dan, apabila berlaku, mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.
***Act* (peningkatan dan pemeliharaan SMKI)**	Mengambil tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI.

Alur Model SMKI

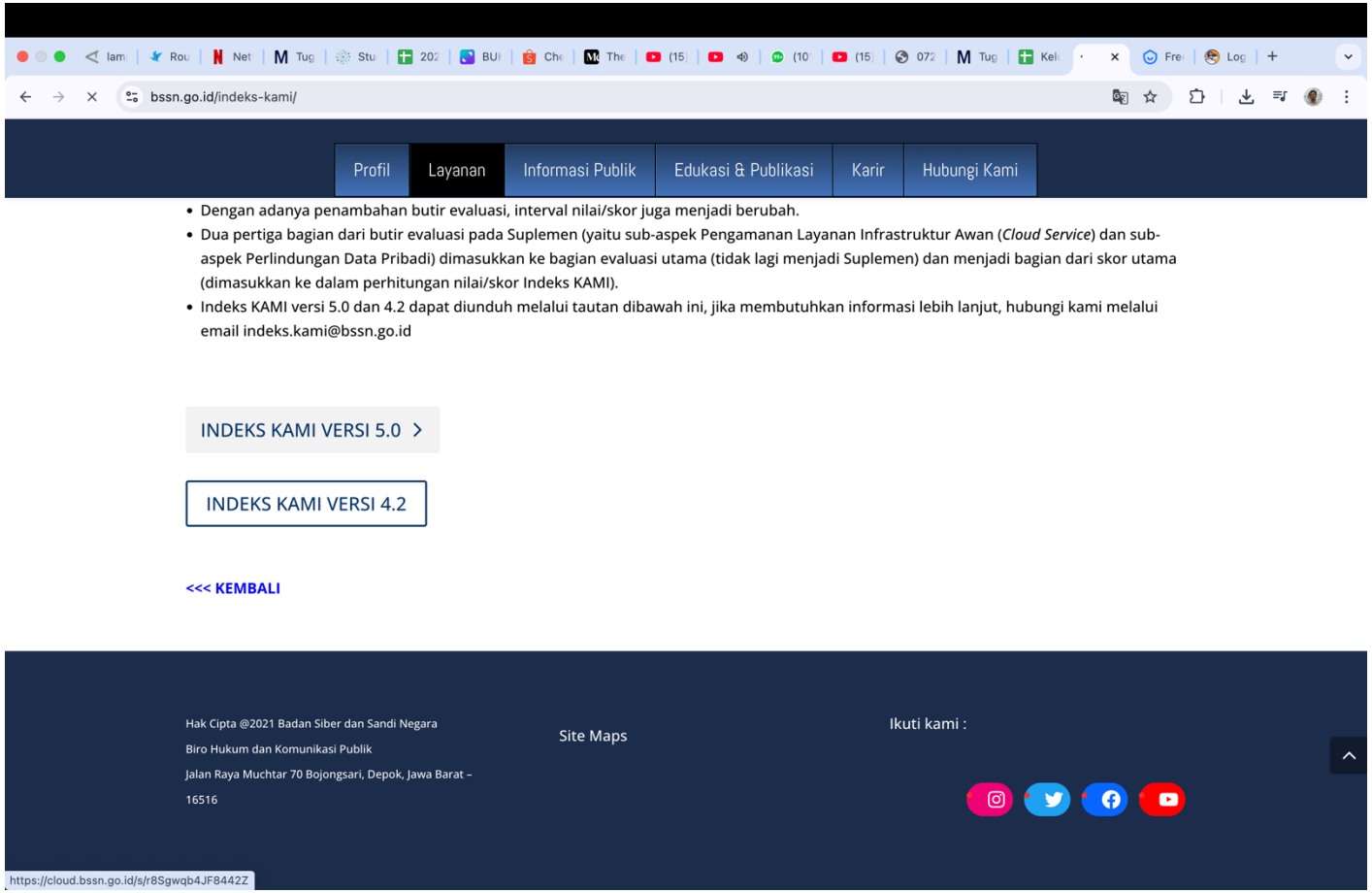
Organisasi Fungsional SMKI





Manfaat SMKI

download


bssn.go.id/indeks-kami/
Profil
Layanan
Informasi Publik
Edukasi & Publikasi
Karir
Hubungi Kami
• Dengan adanya penambahan butir evaluasi, interval nilai/skor juga menjadi berubah.
• Dua pertiga bagian dari butir evaluasi pada Suplemen (yaitu sub-aspek Pengamanan Layanan Infrastruktur Awan (Cloud Service) dan sub-aspek Perlindungan Data Pribadi) dimasukkan ke bagian evaluasi utama (tidak lagi menjadi Suplemen) dan menjadi bagian dari skor utama (dimasukkan ke dalam perhitungan nilai/skor Indeks KAMI).
• Indeks KAMI versi 5.0 dan 4.2 dapat diunduh melalui tautan dibawah ini, jika membutuhkan informasi lebih lanjut, hubungi kami melalui email indeks.kami@bssn.go.id
INDEKS KAMI VERSI 5.0 >
INDEKS KAMI VERSI 4.2
<<< KEMBALI
Hak Cipta @2021 Badan Siber dan Sandi Negara
Biro Hukum dan Komunikasi Publik
Jalan Raya Muchtar 70 Bojongsari, Depok, Jawa Barat – 16516
Site Maps
Ikuti kami :
https://cloud.bssn.go.id/s/r8Sgwqb4JF8442Z

Ruang Lingkup

Terima Kasih