DIGITAL TALENT SCHOLARSHIP

PEMAHAMAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS SNI ISO/IEC 27001:2013

Materi 1 – Pengantar Sistem Manajemen Keamanan Informasi

KOMINFO Badan Penelitian dan Pengembangan Sumber Daya Manusia

#JADIJAGOANDIGITAL

Profil Pengajar

AKBAR ARYANTO

- Join BSN 2005
- Koordinator Kelompok Substansi Infrastruktur dan Keamanan Informasi PUSDATIN – BSN
- Universitas Gunadarma 1998
- University of Twente – Netherlands 2016
- Universitas Gunadarma 2021
- Assesor SMKI 27001:2013 – KAN
- Lead Auditor SMKI 27001:2013
- akbar@bsn.go.id

Indra Hikmawan

- S1 Sistem Informasi Universitas Gunadarma
- Pranata Komputer Ahli Pertama Pusat Data dan Sistem Informasi BSN
- Auditor & Implementer SNI ISO/IEC 27001:2013
- Indra.hikmawan@bsn.go.id

SMKI

Standar

SNI

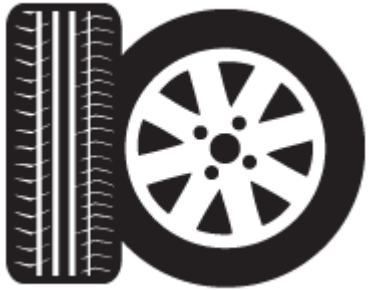
Apa itu standar..?

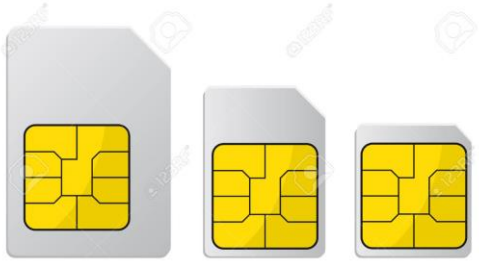
- Sepeda motor tidak ambruk;
- Secara sederhana memiliki fungsi untuk menopang beban kendaraan saat sedang parkir;
- Efisiensi ruang parkir;

Apa itu standar..?

- Kepastian untuk pelanggan;
- Jaminan kepuasan pelanggan;
- Kemudahan ekspor;

Contoh Barang standar





Definisi Standar Berdasarkan UU No. 20 SPK Tahun 2014

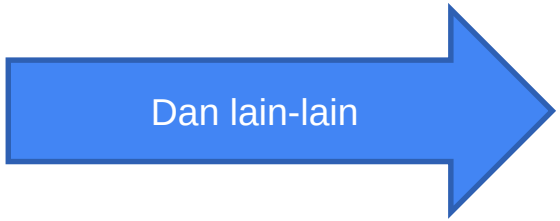
Standar adalah persyaratan teknis atau sesuatu yang dibakukan, termasuk tata cara dan metode yang disusun berdasarkan konsensus semua pihak/Pemerintah/keputusan internasional yang terkait dengan memperhatikan syarat keselamatan, keamanan, kesehatan, lingkungan hidup, perkembangan ilmu pengetahuan dan teknologi, pengalaman, serta perkembangan masa kini dan masa depan untuk memperoleh manfaat yang sebesar-besarnya.


ISO


SNI

Mengapa perlu standar ?

- Melindungi konsumen, pelaku usaha dan masyarakat
- Meningkatkan jaminan mutu, efisiensi produksi, dan kemampuan pelaku usaha
- Bahasa dalam semua bidang, baik perdagangan, industri, pendidikan, dan pengujian
- Meningkatkan kepastian dan efisiensi transaksi perdagangan barang dan jasa baik dalam negeri maupun luar negeri
- Meningkatkan nilai dari suatu produk, jasa, penelitian di dalam negeri maupun luar negeri.



Apa itu Keamanan Informasi

Keamanan Informasi adalah Penjagaan terhadap
Kerahasiaan (**Confidentiality**),
Keutuhan (**Integrity**) dan
Ketersediaan (**Availability**) atas informasi.

- SNI ISO/IEC 27000:2013 -

Apa Itu Informasi

- Sesuatu (data) yang **memiliki nilai** (bisnis dan operasional) bagi organisasi.
- Sesuatu (data) yang **kritikal bagi operasional** organisasi.
- Infomasi adalah **aset**, seperti aset bisnis penting lainnya, yang memiliki nilai bagi suatu organisasi sehingga pada akhirnya perlu untuk diamankan.

Contoh Informasi

Informasi : Website, Data Masyarakat data Karyawan, perjanjian dan kontrak, data keuangan

Perangkat Lunak : Aplikasi Office, Operating Sistem, Aplikasi Editing, Web aplikasi, Anti virus

Perangkat Keras : Komputer , Laptop, Switch , Printer

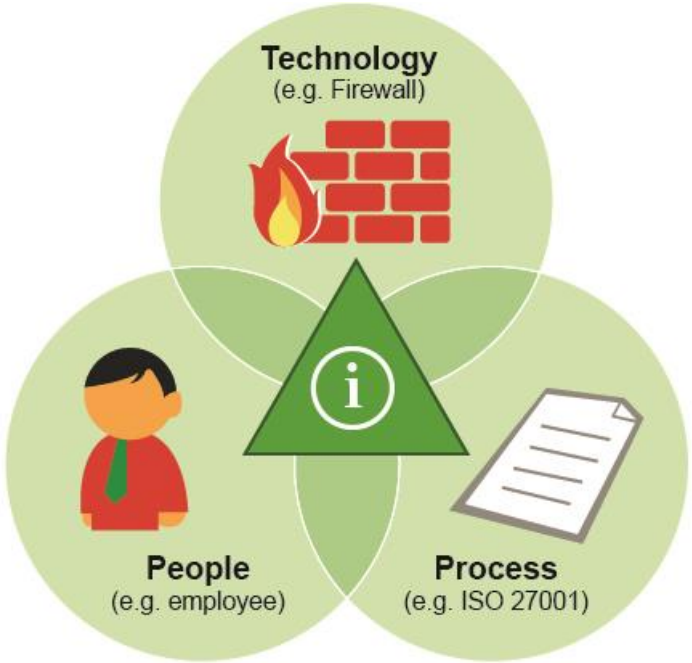
Sarana Pendukung : Listrik, Gedung, Jaringan Internet, Jaringan telepon

Sumber daya Manusia dengan keahliannya

Aset tidak Berwujud : Reputasi, Image Perusahan

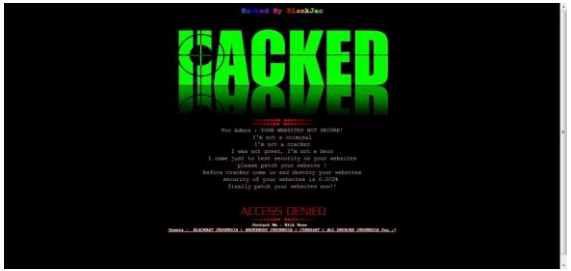
Elemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) **adalah** pendekatan sistematis untuk mengelola informasi perusahaan yang sensitif sehingga tetap aman. Yang di dalam termasuk orang, proses dan sistem TI (Teknologi Informasi) dengan menerapkan proses manajemen resiko.



Serangan Keamaan Infromasi

- Malware (Virus, Worm, Spyware, Keylogger, DOS, DDOS, etc)
- Spam, Phising
- Web Defaced
- Pencurian Data
- Pencurian Hardware



Ancaman Infromasi Lainnya

- Penyalahgunaan Aset
- Lupa membackup
- Kesalahan Konfigurasi
- Benca Alam
- Overheat
- Listrik Padam

Motivasi Dibalik Serangan Cyber

Hanya untuk bersenang-senang

Ketenaran dan popularitas

Kegiatan yang menantang

Keuntungan finansial pribadi

Kecemburuan, kemarahan

Balas dendam

Serangan acak

Ideologis / politis

Dampak Risiko

Reputasi

Finansial

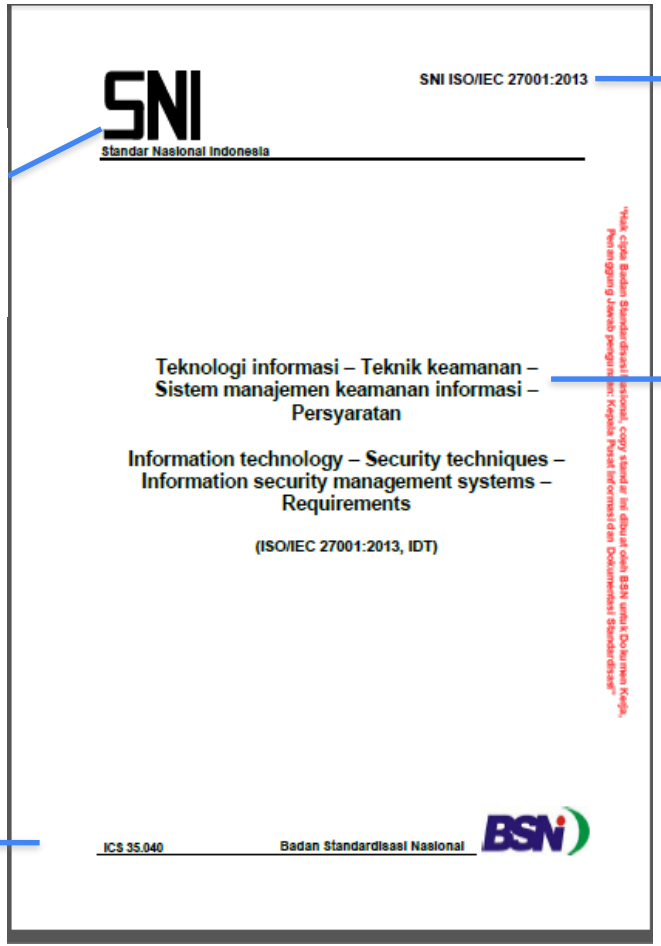
Operasional

Siapa Yang membutuhkan ?
SNI ISO/IEC 27001:2013

Manfaat menerapkan SMKI

- Mengidentifikasi tujuan keamanan informasi
- Melindungi sumberdaya informasi dari gangguan keamanan informasi
- Mempelajari tentang tanggungjawab personil untuk menjaga keamanan informasi
- Merespon insiden keamanan informasi apabila mengalami masalah keamanan informasi.

SNI ISO/IEC 27001:2013


SNI

Standar Nasional Indonesia

SNI ISO/IEC 27001:2013

Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan

Information technology – Security techniques – Information security management systems – Requirements

(ISO/IEC 27001:2013, IDT)

ICS 35.040

Badan Standardisasi Nasional

BSN

Logo Dokumen SNI

Nomor SNI

Judul SNI

Kode International Classification Standards

Struktur SNI ISO/ISO 27001:2013

Klausul 4 - 10 tidak dapat dikecualikan (wajib) dalam sertifikasi SNI ISO/IEC 27001:2013

Terdiri dari 10 klausul dan lampiran Annex, dengan 14 Kelompok Domain dan 114 Kendali (Kontrol)

Struktur SNI ISO/ISO 27001:2013

1. Ruang Lingkup

2. Acuan Normatif

3. Istilah dan Definisi

4. Konteks Organisasi

4.1 Memahami organisasi & kontek
4.2 Memahami kebutuhan
4.3 Penentuan ruang lingkup SMKI
4.4 SMKI

5. Kepemimpinan

5.1 Kepemimpinan & komitmen
5.2 Kebijakan
5.3 Peran organisasi, tanggung jawab & wewenang

6. Perencanaan

6.1 Tindakan untuk menangani resiko & peluang
6.2 Sasaran keamanan informasi & perencanaan untuk mencapaianya

7. Dukungan

7.1 Sumberdaya
7.2 Kompetensi
7.3 Kepedulian
7.4 Komunikasi
7.5 Informasi terdokumentasi

8. Operasi

8.1 Perencanaan & pengendalian operasional
8.2 Penilaian resiko keamanan informasi
8.3 Penanganan resiko keamanan informasi

9. Evaluasi Kinerja

9.1 Pemantauan, pengukuran, analisis & evaluasi
9.2 Audit internal
9.3 Reviu manajemen

10. Perbaikan

10.1 Ketidaksesuaian & tindakan korektif
10.2 Perbaikan berkelanjutan

Lampiran Annex SNI ISO/ISO 27001:2013

SNI ISO/IEC 27001:2013 Control Point and Control Objective		
Annex	**Deskripsi**	**total Kontrol**
A5	Kebijakan Keamanan Informasi	**2**
A6	Organisasi Keamanan informasi	**7**
A7	Keamanan Sumber Daya Manusia	**6**
A8	Manajemen Aset	**10**
A9	Kendali Akses	**14**
A10	Kriptografi	**2**
A11	Keamanan Fisik dan Lingkungan	**15**
A12	Keamanan Operasi	**14**
A13	Keamanan Komunukasi	**7**
A14	Akuisisi, Pengembangan dan Perawatan Sistem	**13**
A15	Hubungan Pemasok	**5**
A16	Manajemen Insiden Keamanan Informasi	**7**
A17	Aspek Keamanan Informasi dari Manajemen Keberlangsungan	**4**
A18	Kesesuaian	**8**
Total Kontrol		**114**

Lampiran Annex SNI ISO/ISO 27001:2013

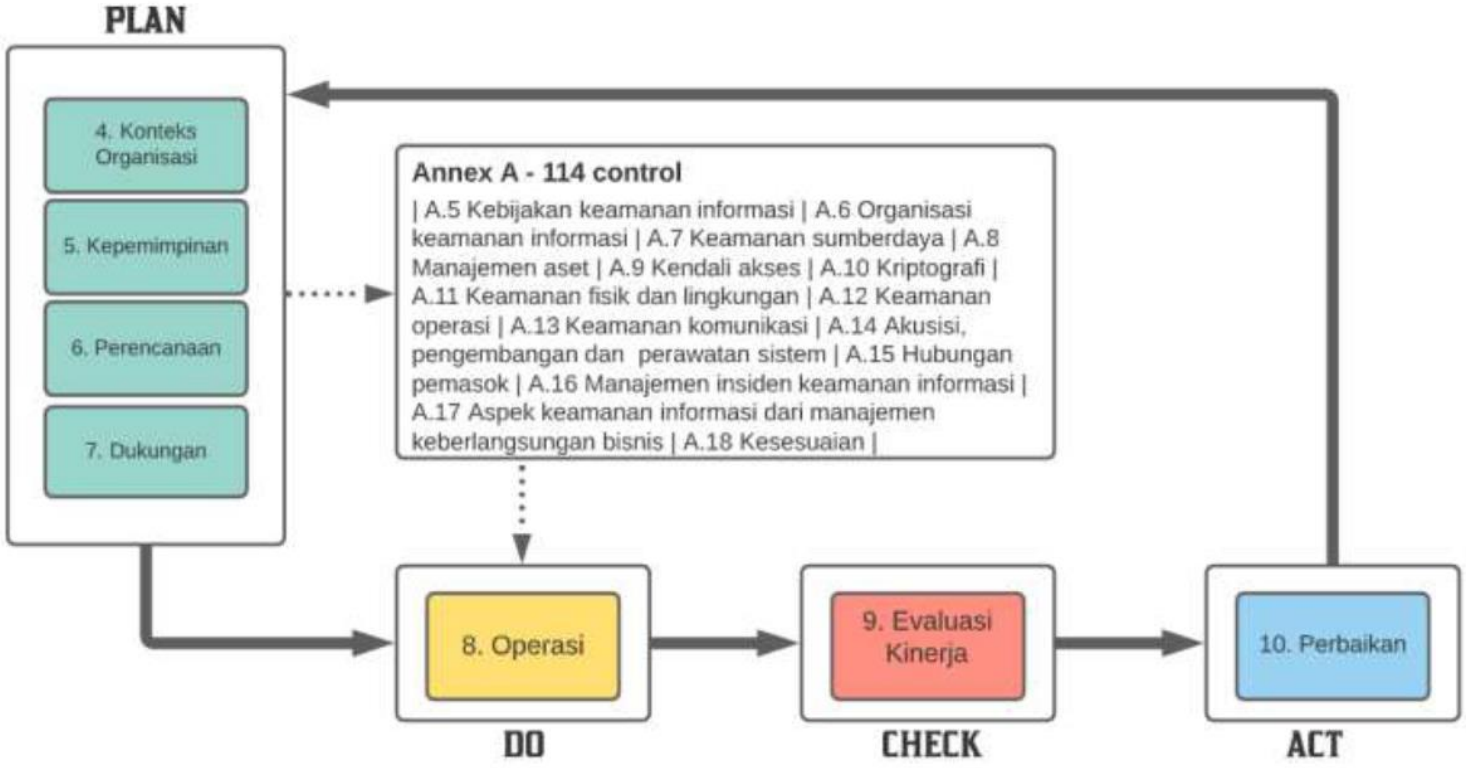
Lampiran A
(normatif)
Acuan untuk sasaran kendali dan kendali

Sasaran kendali dan kendali yang tercantum dalam Tabel A.1 secara langsung berasal dari dan sesuai dengan yang terdaftar di ISO/IEC 27002:2013[1], Klausul 5 hingga klausul 18, dan akan dipergunakan dalam Klausul 6.1.3.

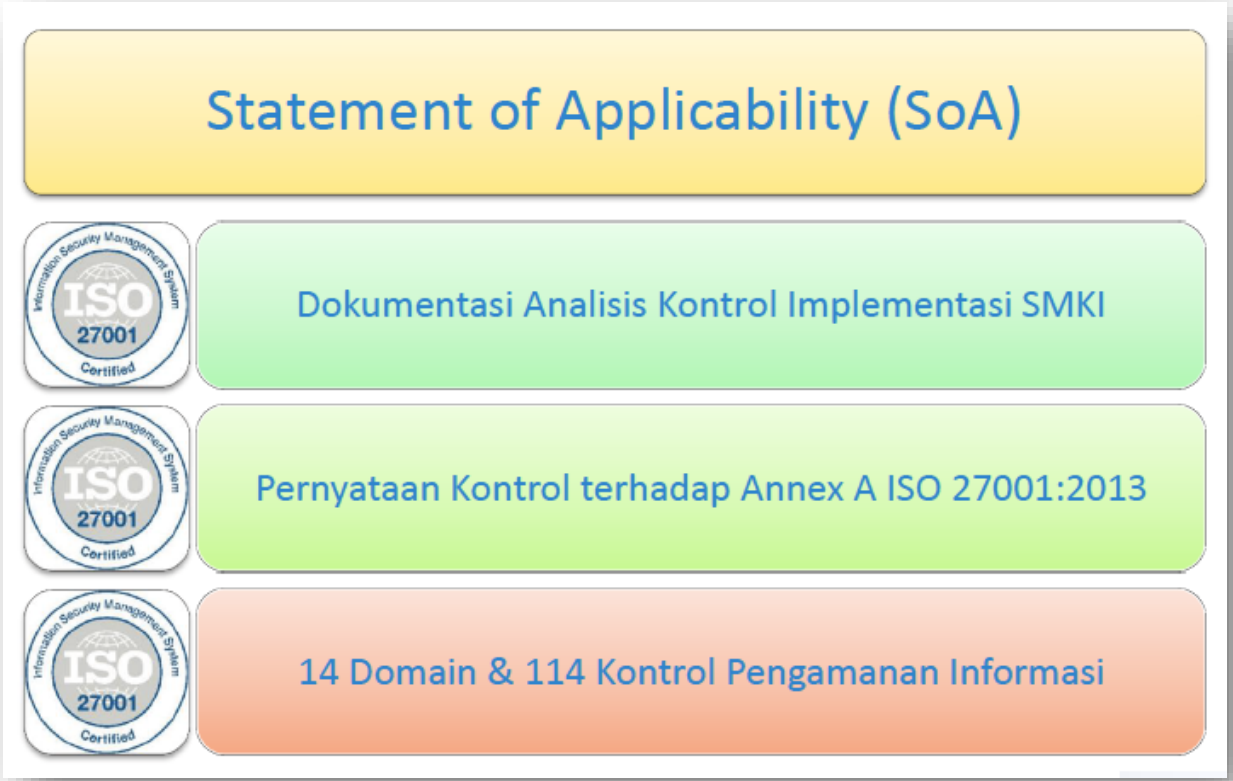
Tabel A.1 — Sasaran kendali dan kendali

A.5 Kebijakan keamanan informasi		
A.5.1 Arahan manajemen untuk keamanan informasi		
Sasaran: Untuk memberikan arah dan dukungan manajemen untuk keamanan informasi sesuai dengan persyaratan bisnis dan regulasi dan hukum yang relevan		
A.5.1.1	Kebijakan untuk keamanan informasi	*Kendali* Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak luar yang terkait.
A.5.1.2	Reviu kebijakan keamanan informasi	*Kendali* Kebijakan untuk keamanan informasi harus direviu pada interval waktu terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan dan keefektifan yang berkelanjutan
A.8 Manajemen aset		
A.8.1 Tanggung jawab terhadap aset		
Sasaran: Untuk mengenali aset organisasi dan menetapkan tanggung jawab perlindungan yang sesuai.		
A.8.1.1	Inventaris aset	*Kendali* Aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan inventaris dari aset-aset ini harus dicatat dan dipelihara.
A.8.1.2	Kepemilikan aset	*Kendali* Aset yang dipelihara dalam inventaris harus dimiliki (ada personel yang bertanggung jawab).
A.8.1.3	Penggunaan yang dapat diterima (*acceptable use*) atas aset	*Kendali* Aturan untuk penggunaan yang dapat diterima atas informasi dan aset yang berhubungan dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi, didokumentasi dan diimplementasikan.
A.8.1.4	Pengembalian aset	*Kendali* Semua pegawai dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang dikuasainya ketika terjadi penghentian kepegawaian, kontrak atau perjanjian mereka.
A.10 Kriptografi		
A.10.1 Kendali kriptografi		
Sasaran: Untuk memastikan penggunaan kriptografi secara tepat dan efektif dalam melindungi kerahasiaan (*confidentiality*), keotentikkan (*authenticity*) dan/atau keutuhan (*integrity*) informasi.		
A.10.1.1	Kebijakan terhadap penggunaan kendali kriptografi	*Kendali* Kebijakan terhadap penggunaan kendali kriptografi untuk perlindungan informasi harus dikembangkan dan diimplementasikan.
A.10.1.2	Manajemen kunci	*Kendali* Kebijakan terhadap penggunaan, perlindungan dan masa hidup kunci kriptografi harus dikembangkan dan diimplementasikan dalam keseluruhan siklus hidupnya.
A.11 Keamanan fisik dan lingkungan		

Siklus PDCA SNI ISO/ISO 27001:2013



Statement of Applicability (SOA)



Pernyataan Pemberlakuan/ Statement of Applicability

Annex 27001	Judul	Y/T	
A.5	Kebijakan Keamanan informasi		
A.5.1	Arahan Manajemen untuk keamaan informasi		
A.5.1.1	Kebijakan untuk keamanan informasi	Y	Dokumen pedoman kemaan informasi disetujui oleh direksi dan dikomunikasikan kepada karyawan
A.5.1.2	Reviu kebijakan kemaan informasi	Y	Dilakukan minimum 1 tahun sekali dalam rapat yang melibatkan majemen

Keuntungan menerapkan SNI ISO/IEC 27001:2013

- ✓ Membuat pengaruh positif dalam hal citra perusahaan, nilai, dan persepsi yang baik dari pihak lain.
- ✓ Memastikan bahwa organisasi memiliki kontrol terkait keamanan informasi terhadap lingkungan proses bisnisnya yang mungkin menimbulkan risiko atau gangguan.
- ✓ Dapat digabung atau dikombinasikan dengan sistem manajemen lainnya seperti SNI ISO 9001, SNI ISO 14000, SNI ISO 20000-1, SNI ISO 37001, SNI ISO 38500, ITIL, COBIT dll.
- ✓ Salah satu standar pengamanan informasi yang diakui di seluruh dunia.
- ✓ Patuh terhadap hukum dan undang-undang seperti UU ITE, dll.
- ✓ Meningkatkan awareness terhadap keamanan informasi pada pegawai/karyawan.

Landasan Pelaksanaan Evaluasi SPBE

PERPRES 95/2018

PERMENPANRB 5/2018

Pedoman **Evaluasi SPBE** digunakan sebagai panduan dalam melakukan penilaian/evaluasi SPBE untuk **mengukur kemajuan pelaksanaan Sistem Pemerintahan Berbasis Elektronik** pada Instansi Pusat dan Pemerintah Daerah.

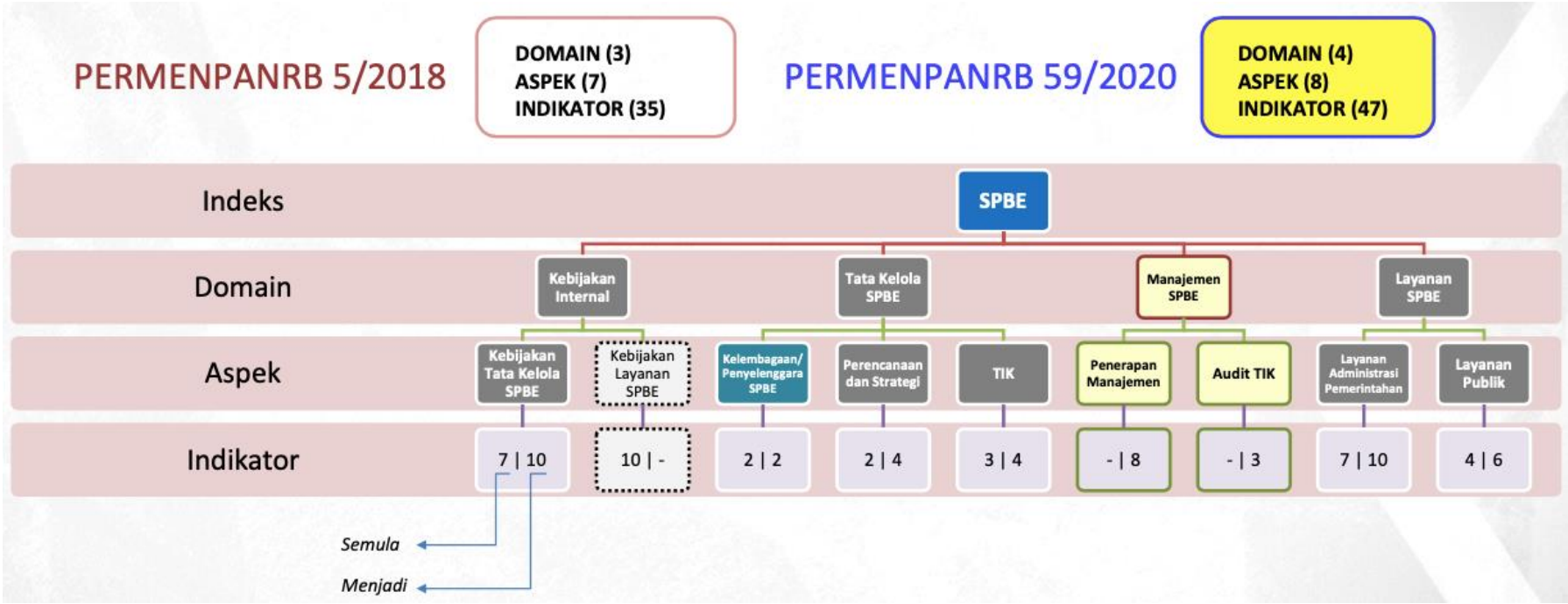
REVISI TERHADAP PERMENPANRB 5/2018

PermenPANRB No. 5 Tahun 2018 terbit lebih dulu (9 bulan 11 hari) sebelum Perpres 95 Tahun 2018 terbit.

Beberapa **amanat** Perpres 95 Tahun 2018 yang **belum terakomodasi** dalam PermenPANRB No. 5 Tahun 2018, antara lain:

a. Arsitektur SPBE (Pasal 6–12)
b. Peta Rencana SPBE (Pasal 13–19)
c. Jaringan Intra Pemerintah (Pasal 32)
d. Sistem Penghubung Layanan (Pasal 33)
e. Pembangunan Aplikasi Terpadu (Pasal 34–39)
f. Keamanan SPBE (Pasal 40–41)
g. Manajemen SPBE: Manajemen Risiko, Manajemen Data, Manajemen Aset TIK, Manajemen Keamanan Informasi, Manajemen Layanan, Manajemen SDM SPBE, Manajemen Perubahan, Manajemen Pengetahuan (Pasal 46–54)
h. Audit TIK: Audit Aplikasi, Audit Infrastruktur, Audit Keamanan (Pasal 55–58)

Struktur Penilaian



#JADIJAGOANDIGITAL

TERIMA KASIH

digitalent.kominfo

DTS_kominfo

digitalent.kominfo

digital talent scholarship