



Audit Keamanan SPBE

Government Transformation Academy

Profil Pengajar

<Nama Pengajar>

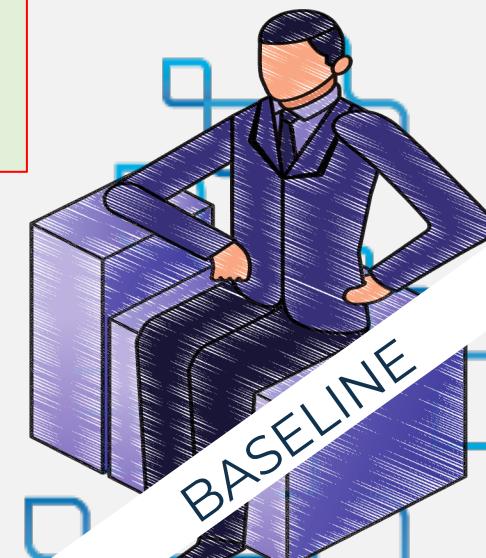
Profil....



DASAR REGULASI AUDIT KEAMANAN SPBE

DASAR

- Perpres 95 Tahun 2018 tentang SPBE (Pasal 58) ;
- Perpres 132 Tahun 2022 tentang Arsitektur SPBE;
- Peraturan BSSN No.4 Tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE
- Permenkominfo No. 16 Tahun 2022 tentang Kebijakan Umum Audit TIK
- Rancangan Peraturan BSSN tentang Standar dan Tata Cara Audit Keamanan SPBE

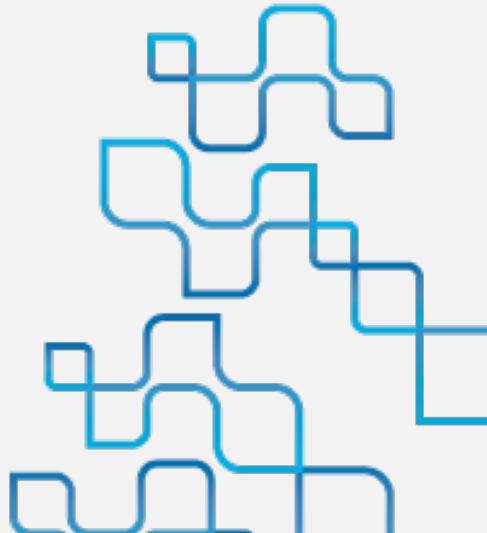


OUTLINE MATERI



PEMAHAMAN AUDIT KEAMANAN SPBE

Informasi atau Ketentuan
Terkait Audit Keamanan
SPBE yang dilakukan pada
Aplikasi Umum dan Khusus



OUTLINE MATERI

PEMAHAMAN

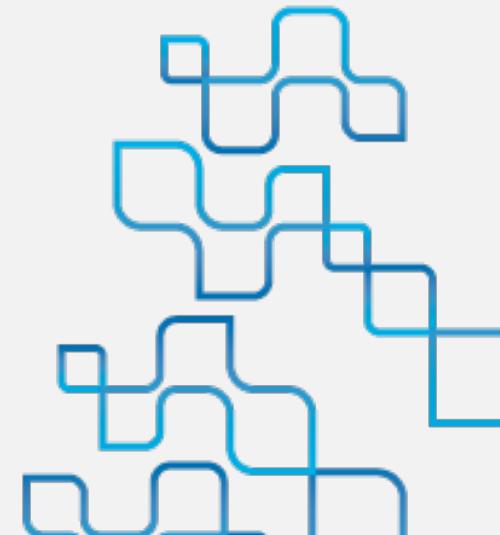
1

AUDIT KEAMANAN SPBE

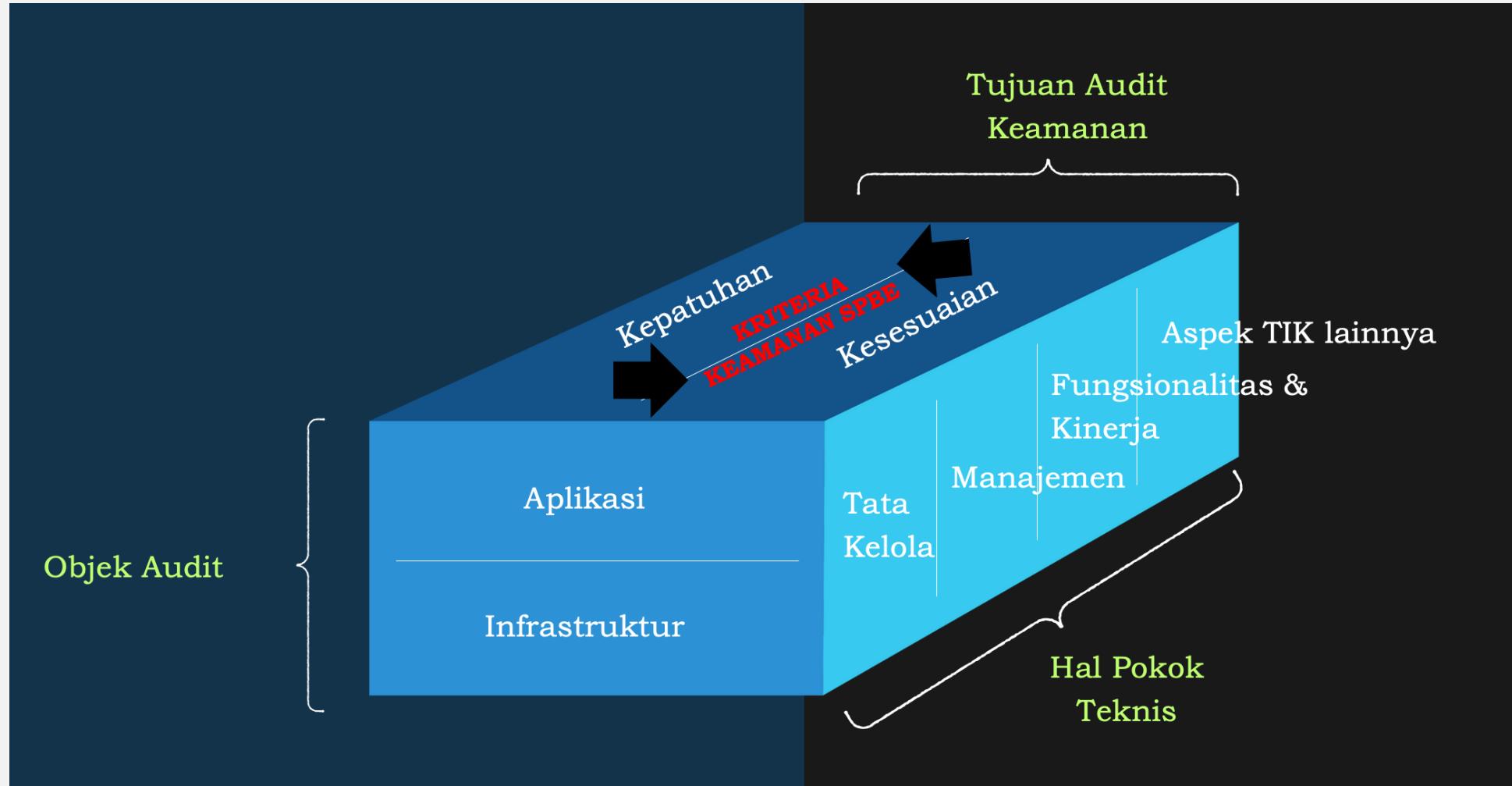
Informasi atau Ketentuan Terkait Audit Keamanan SPBE yang dilakukan pada Aplikasi Umum dan Khusus



AUDIT

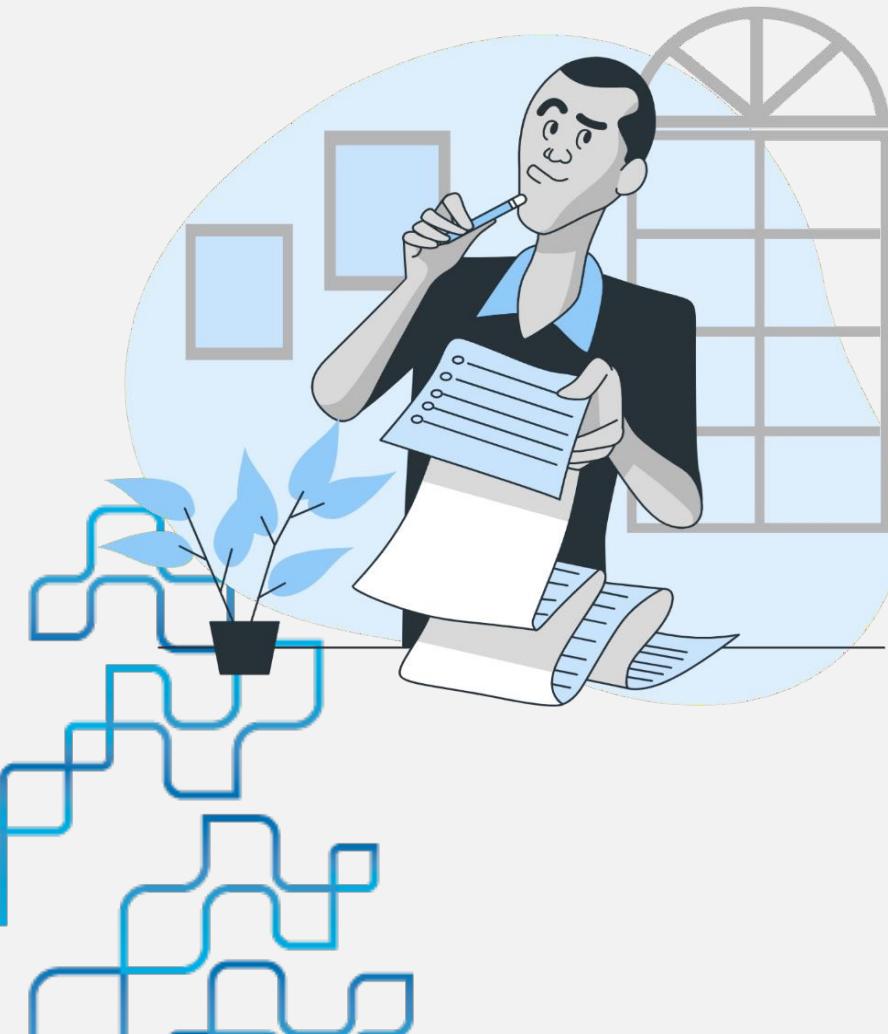


KETENTUAN AUDIT KEAMANAN SPBE



Sumber: 1. Peraturan Presiden No 95 Tahun 2018 tentang SPBE
2. Permenkominfo No.16 Tahun 2022 tentang Kupatik

AUDIT TIK SPBE

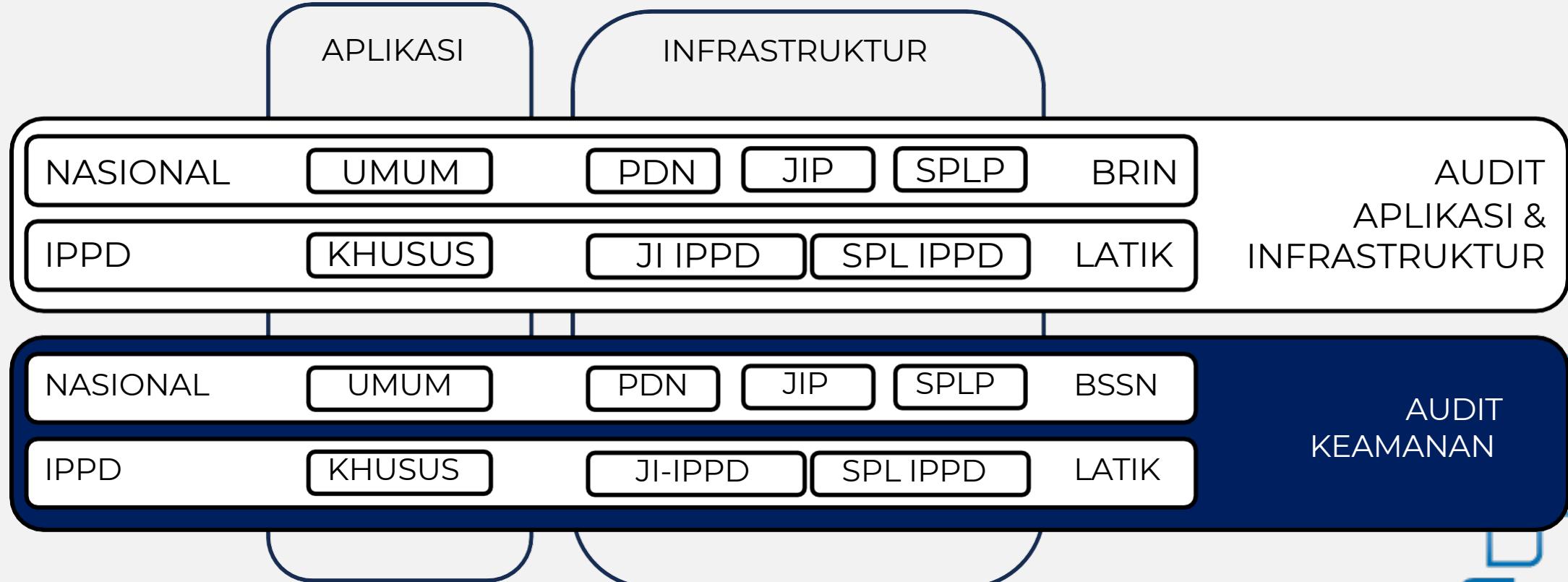


Pasal 1 Perpres Nomor 95 Tahun 2018

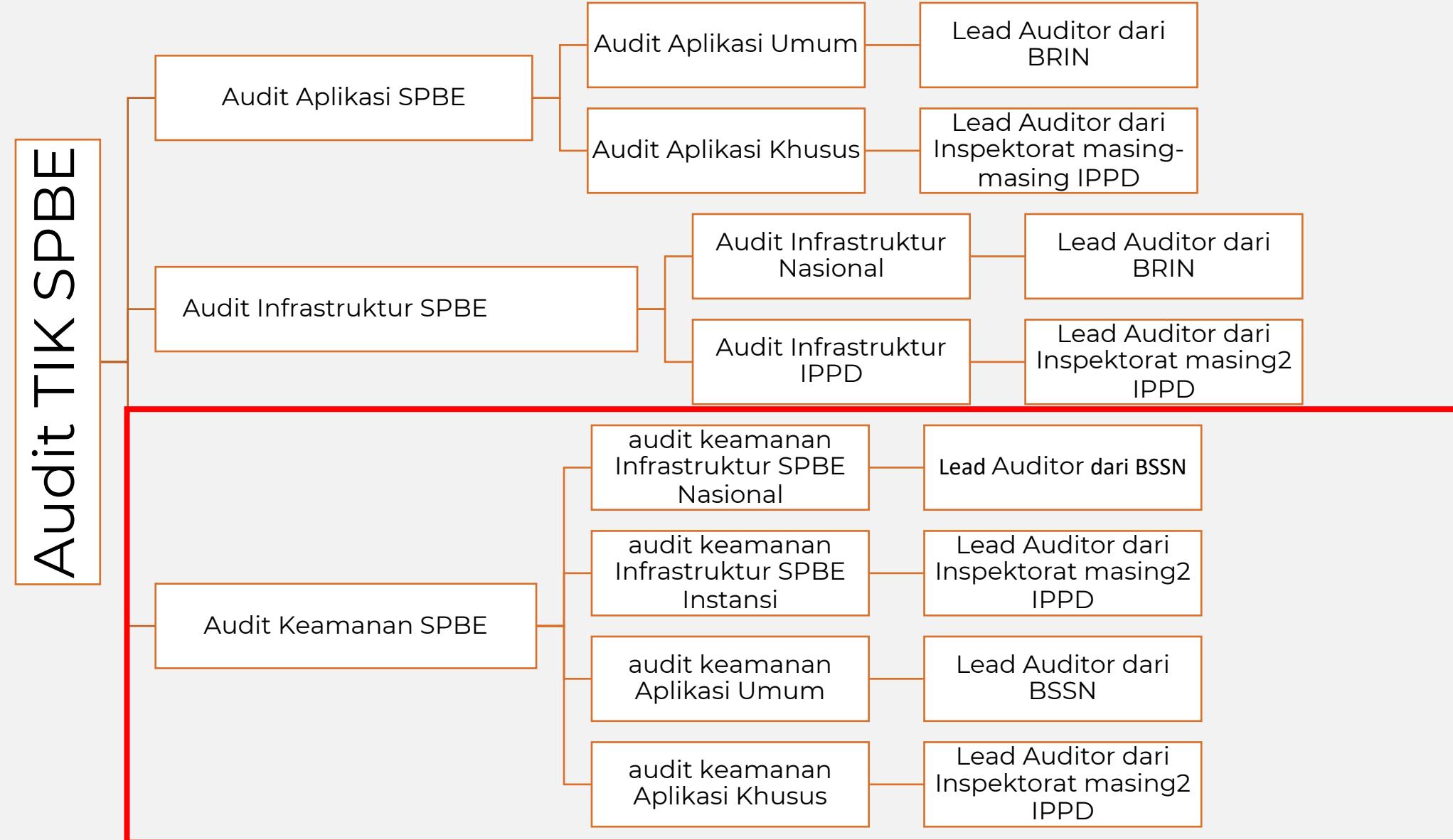
Audit Teknologi Informasi dan Komunikasi adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk **menetapkan tingkat kesesuaian** antara teknologi informasi dan komunikasi **dengan kriteria yang telah ditetapkan.**



SEMESTA AUDIT TIK



PENANGGUNG JAWAB/PELAKSANA AUDIT TIK



UNIT KERJA

PELAKSANA AUDIT INTERNAL

- (1) Audit Keamanan SPBE internal sebagaimana dimaksud pada RPB STA dilaksanakan dengan tahapan:
 - a. perencanaan;
 - b. pelaksanaan;
 - c. pelaporan; dan
 - d. pemantauan tindak lanjut.
- (2) Audit Keamanan SPBE internal sebagaimana dimaksud pada RPB STA dilaksanakan secara periodik oleh auditor pada unit kerja Instansi Pusat atau Pemerintah Daerah yang melaksanakan tugas dan fungsi di bidang pengawasan intern.
- (3) Unit kerja Instansi Pusat atau Pemerintah Daerah yang melaksanakan tugas dan fungsi di bidang pengawasan intern sebagaimana dimaksud pada RPB STA dapat melibatkan pegawai aparatur sipil negara dari unit kerja lain yang memiliki kompetensi:
 - a. Audit TIK; dan/atau
 - b. audit keamanan informasi.
- (4) Kompetensi Audit sebagaimana dimaksud pada RPB STA dibuktikan dengan sertifikat pelatihan audit TIK dan/atau audit keamanan informasi.
- (5) Pelatihan audit sebagaimana dimaksud pada RPB STA diselenggarakan oleh Badan atau lembaga pelatihan lain yang mendapat pengakuan dari Badan.

AUDIT TIK EKSTERNAL

AUDIT INFRASTRUKTUR SPBE

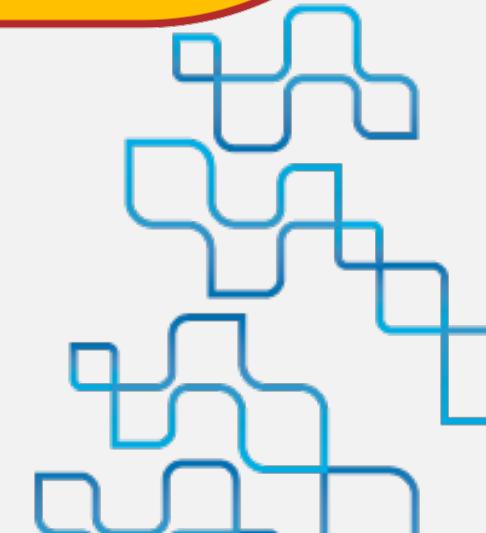
- Infrastruktur SPBE Nasional di audit setiap tahun oleh BRIN
- Infrastruktur SPBE instansi Pusat dan Pemerintah Daerah diaudit setiap dua tahun oleh Lembaga audit TIK
- Koordinasi dengan kementerian Kominfo

AUDIT KEAMANAN

- Audit Keamanan pada infrastruktur SPBE Nasional dan Aplikasi Umum dilakukan setiap tahun oleh BSSN
- Audit Keamanan pada infrastruktur SPBE Instansi Pusat dan Pemda serta Aplikasi Khusus dilakukan minimal 1 (satu) kali dalam 2 (dua) tahun oleh Lembaga Audit TIK

AUDIT APLIKASI SPBE

- Aplikasi umum diaudit setiap tahun oleh BRIN
- Aplikasi khusus di audit setiap dua tahun oleh Lembaga Audit TIK
- Koordinasi dengan Kementerian Kominfo



AUDIT TIK INETRNAL

AUDIT INFRASTRUKTUR SPBE

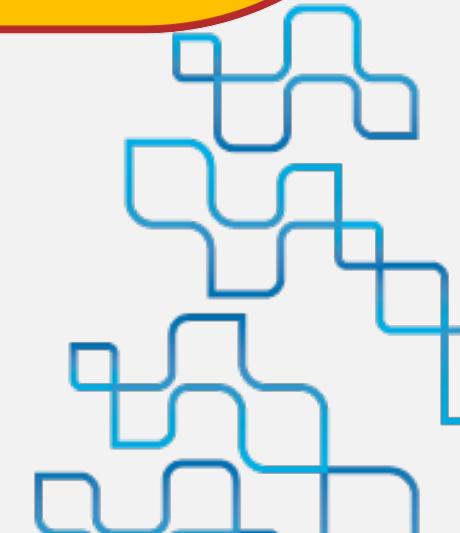
- Infrastruktur SPBE instansi Pusat dan Pemerintah Daerah diaudit setiap dua tahun oleh Unit Pengawasan
- Koordinasi dengan BRIN

AUDIT KEAMANAN

- Audit Keamanan SPBE pada **aplikasi khusus** dan **infrastruktur SPBE** untuk kebutuhan internal di **Instansi Pusat dan Pemda** masing-masing dilakukan minimal 1 (satu) kali dalam 2 (dua) tahun oleh Unit Kerja Pengawasan
- Kooordinasi dengan BSSN

AUDIT APLIKASI SPBE

- Aplikasi Khusus diaudit setiap tahun oleh Unit Kerja Pengawasan
- Koordinasi dengan BRIN



PRINSIP/CAKUPAN KEAMANAN SPBE

PASAL 41 PERPRES NO.95 TAHUN 2018



PENJAMINAN KERAHASIAAN

Penetapan klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan/enkripsi dan kriptografi.

KEUTUHAN

Pendeteksian modifikasi dan tanda tangan elektronik tersertifikasi.

KETERSEDIAAN

Penyediaan cadangan, perencanaan untuk menjamin data dan informasi dapat selalu diakses, dan pemulihan.

KEASLIAN

Penyediaan mekanisme verifikasi, validasi dan hush function.

KENIRSANGKALAN (NON-REPUDIATION)

Penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.

NEXT OUTLINE MATERI

KRITERIA DAN KONTROL KEAMANAN



KRITERIA

Kriteria yaitu berbagai peraturan perundangan-perundangan dan/atau kebijakan, prosedur, dan instruksi kerja, serta standar dan praktik-praktik terbaik, yang digunakan oleh Auditor TIK untuk melakukan evaluasi dan pengujian atas pengendalian intern TIK, manajemen risiko TIK dan tata kelola TIK

(Peraturan Menteri Kominfo 16/2022)



KONTROL KEAMANAN

Sekumpulan aktivitas keamanan yang harus didefinisikan dan dilaksanakan. Kontrol keamanan diturunkan dari kriteria audit keamanan.



KRITERIA

AUDIT KEAMANAN SPBE

terkait Keamanan SPBE dan pelindungan privasi.



merupakan kebijakan umum berupa undang-undang yang mengatur lebih luas kepentingan masyarakat, pelaku usaha, & pihak-pihak terkait.

Contoh :

UU No. 27 Tahun 2022 tentang PDP, Perpres No. 95 Tahun 2018 tentang SPBE

merupakan kebijakan yang menjelaskan suatu pengaturan berupa peraturan menteri dan peraturan badan yang berlaku bagi semua IPPD

Contoh :

Peraturan BSSN No. 4 Tahun 2021, Permenkominfo No. 16 Tahun 2022

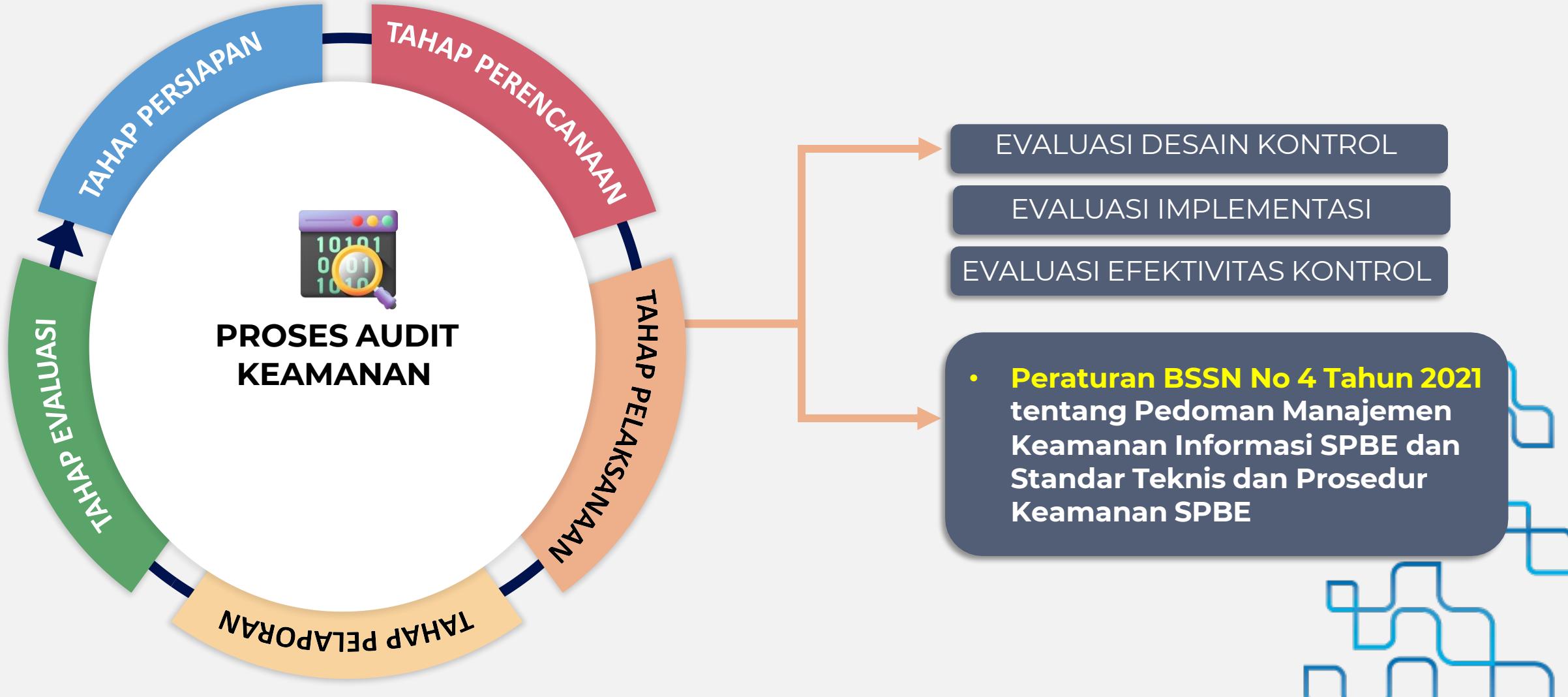
merupakan kebijakan internal Instansi Pusat dan Pemerintah Daerah terkait.

Contoh :

Kebijakan Sistem Manajemen Keamanan Informasi milik IPPD

Selain kriteria tersebut, **dapat** memperhatikan pada **standar nasional** yang berlaku di Indonesia. Dalam hal standar nasional belum tersedia, pelaksanaan Audit Keamanan SPBE **dapat** memperhatikan pada **standar internasional**.

PROSES AUDIT KEAMANAN APLIKASI UMUM DAN INFRASTRUKTUR SPBE NASIONAL



TAHAP PERSIAPAN

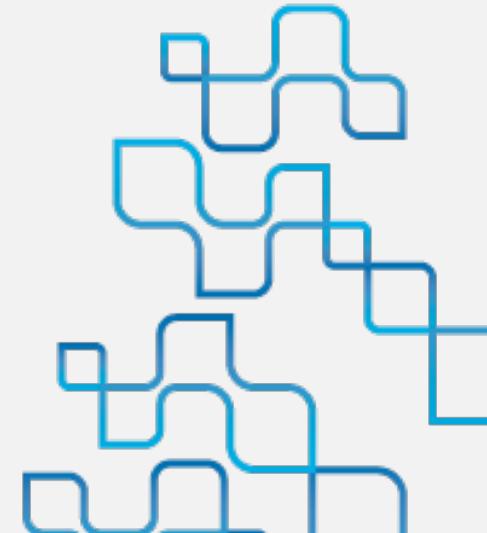
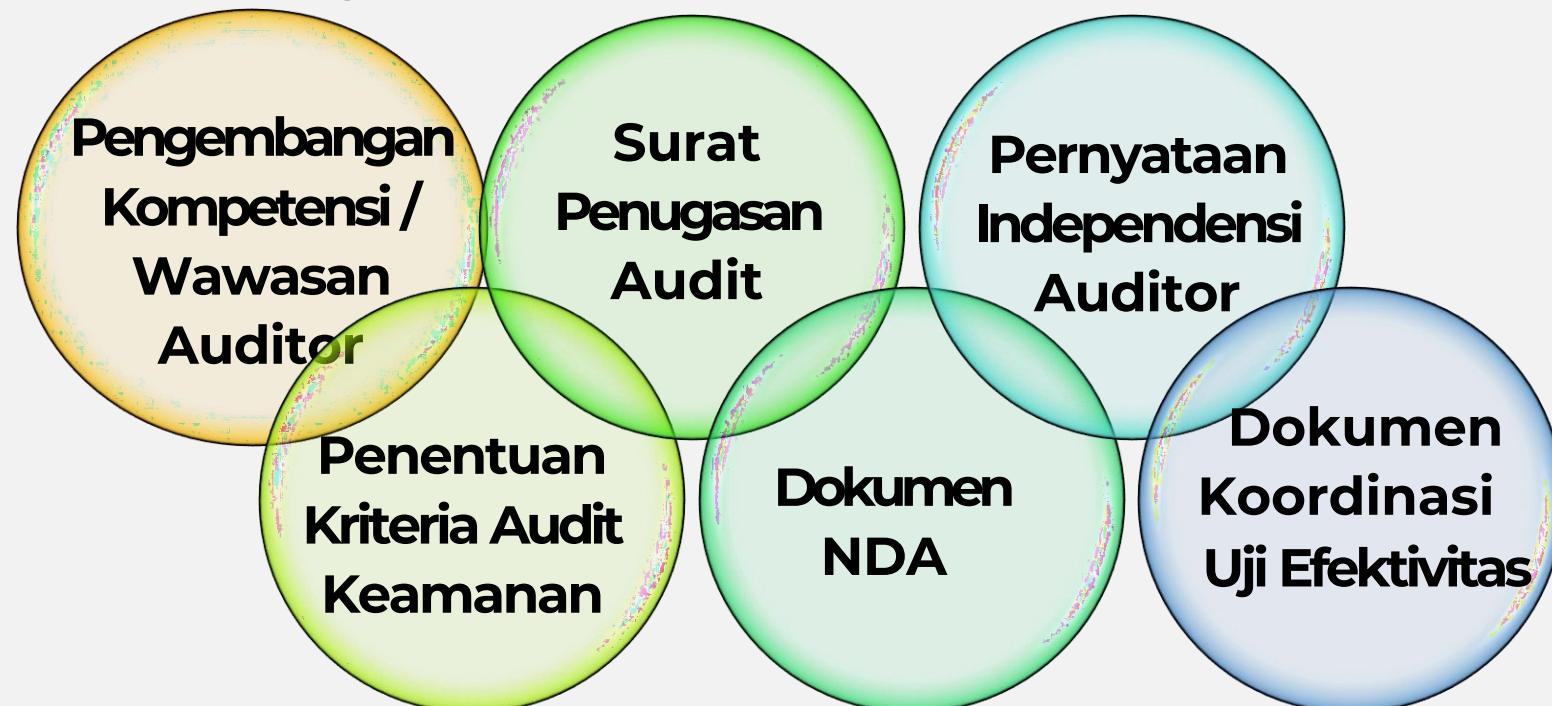


TUJUAN TAHAP PERSIAPAN

Tujuan Tim Auditor melaksanakan kegiatan ini adalah untuk mempersiapkan pelaksanaan Audit Keamanan Aplikasi Khusus/Infra SPBE dengan baik dan sesuai dengan acuan peraturan perundang-undangan



KEGIATAN TAHAP PERSIAPAN



KEBUTUHAN DOKUMEN AWAL AUDIT KEAMANAN APLIKASI/INFRA SPBE

1. Surat perintah/tugas tim audit beserta PIC yang ditunjuk
2. Dokumen yang menjelaskan informasi mengenai aplikasi yang akan di audit (mulai dari perencanaan, pengoperasian, pengembangan, dan pemantauan aplikasi)
3. Dokumen yang menjelaskan proses bisnis dari aplikasi
4. Dokumen yang menjelaskan informasi mengenai infrastruktur aplikasi
5. Dokumen yang menjelaskan prosedur-prosedur terkait dengan aplikasi yang telah disusun serta dijalankan
6. Dokumen yang menjelaskan tugas dan fungsi pihak-pihak yang berkaitan dengan aplikasi
7. Dokumen yang memuat analisis risiko terkait dengan aplikasi dan pendukung

TAHAP PERENCANAAN

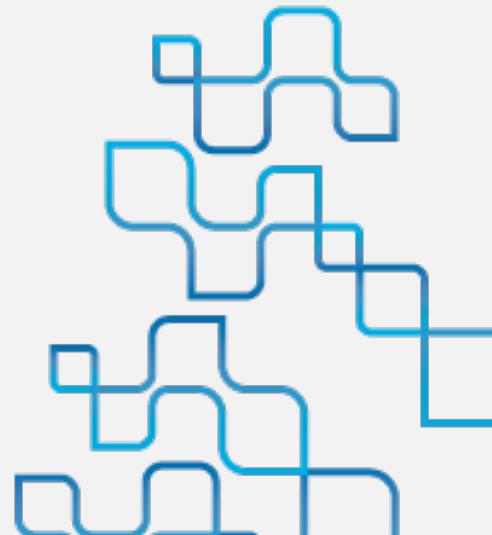
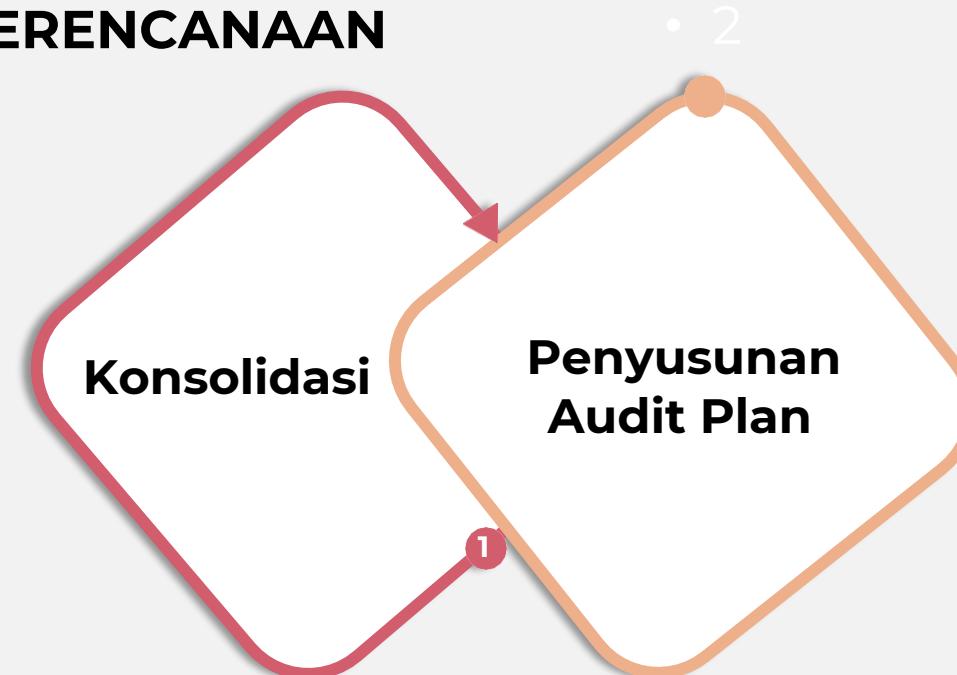


TUJUAN TAHAP PERENCANAAN

Tujuan Tim Auditor melaksanakan kegiatan ini adalah untuk merencanakan pelaksanaan Audit Keamanan Aplikasi Khusus/Infra SPBE dengan baik dalam menentukan ruang lingkup dan metodologi audit keamanan



KEGIATAN TAHAP PERENCANAAN

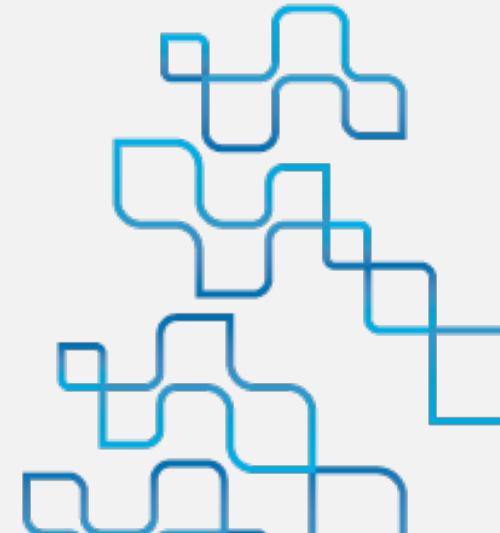
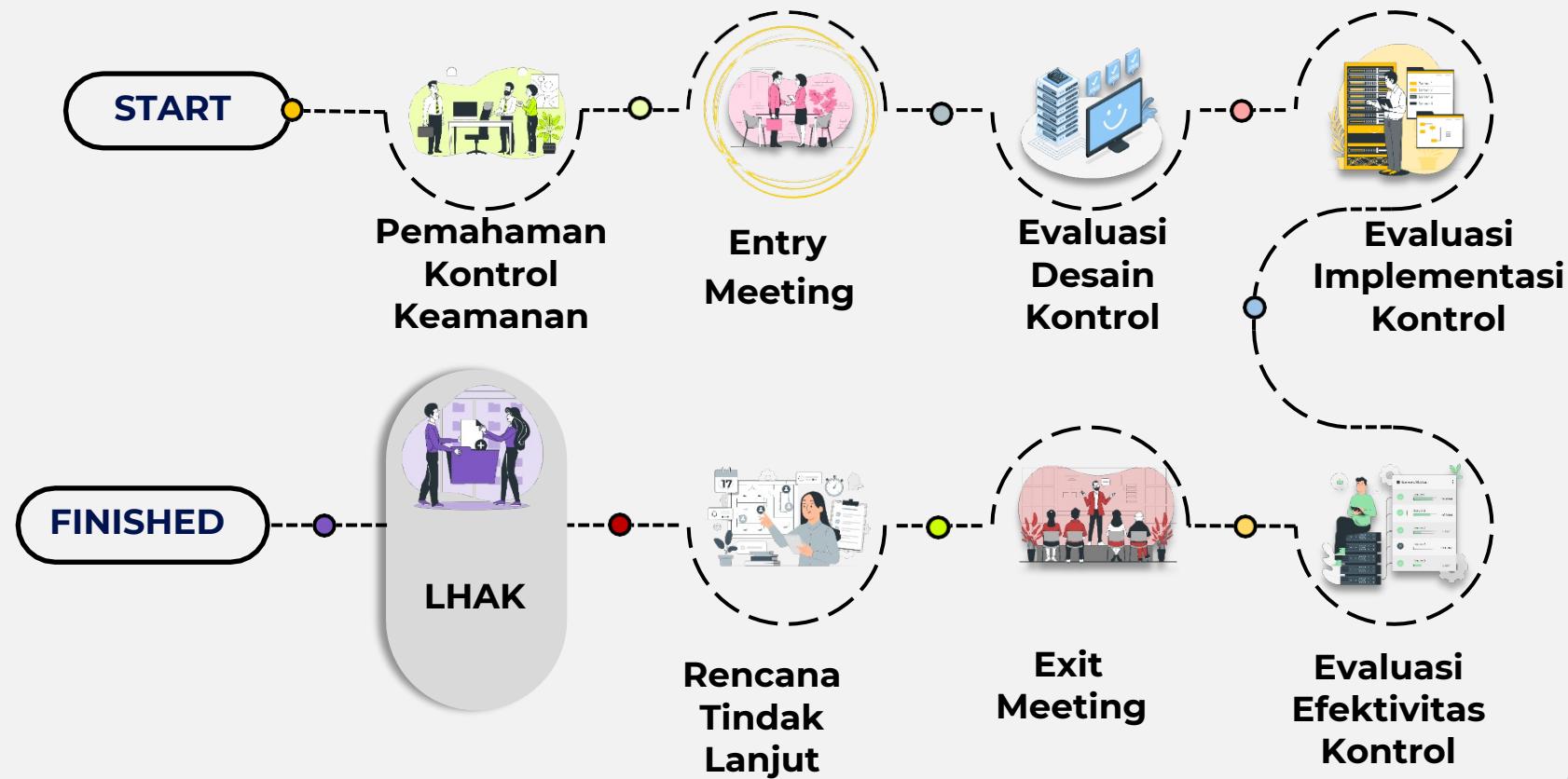


TAHAP PELAKSANAAN



TUJUAN TAHAP PELAKSANAAN

Tujuan dilaksanakan kegiatan ini adalah untuk mendapatkan kesimpulan dari setiap tahapan audit yang dilaksanakan. Kesimpulan yang didapat berupa kesesuaian objek yang diaudit dibandingkan dengan kriteria audit dan temuan hasil pelaksanakan aplikasi objek audit



KESIMPULAN PELAPORAN

Kesimpulan dari setiap prosedur pelaksanaan audit memuat kesimpulan dari:

Pemahaman kontrol

Auditor mengidentifikasi informasi terdokumentasi untuk memperoleh pemahaman yang memadai tentang kontrol keamanan SPBE.

Evaluasi desain kontrol keamanan

Auditor memperoleh keyakinan yang memadai bahwa desain kontrol keamanan SPBE telah sesuai dengan kriteria kontrol keamanan SPBE yang digunakan.

Evaluasi implementasi kontrol keamanan

Auditor melakukan langkah-langkah untuk memperoleh keyakinan yang memadai bahwa implementasi kontrol telah sesuai dengan desain kontrol yang ada.

Evaluasi efektivitas

Auditor melakukan langkah-langkah untuk memperoleh keyakinan yang memadai bahwa kontrol keamanan SPBE telah dapat mencapai tujuannya dengan efektif.

MEMADAI

PERLU PENINGKATAN

TIDAK MEMADAI

SESUAI

TIDAK SESUAI

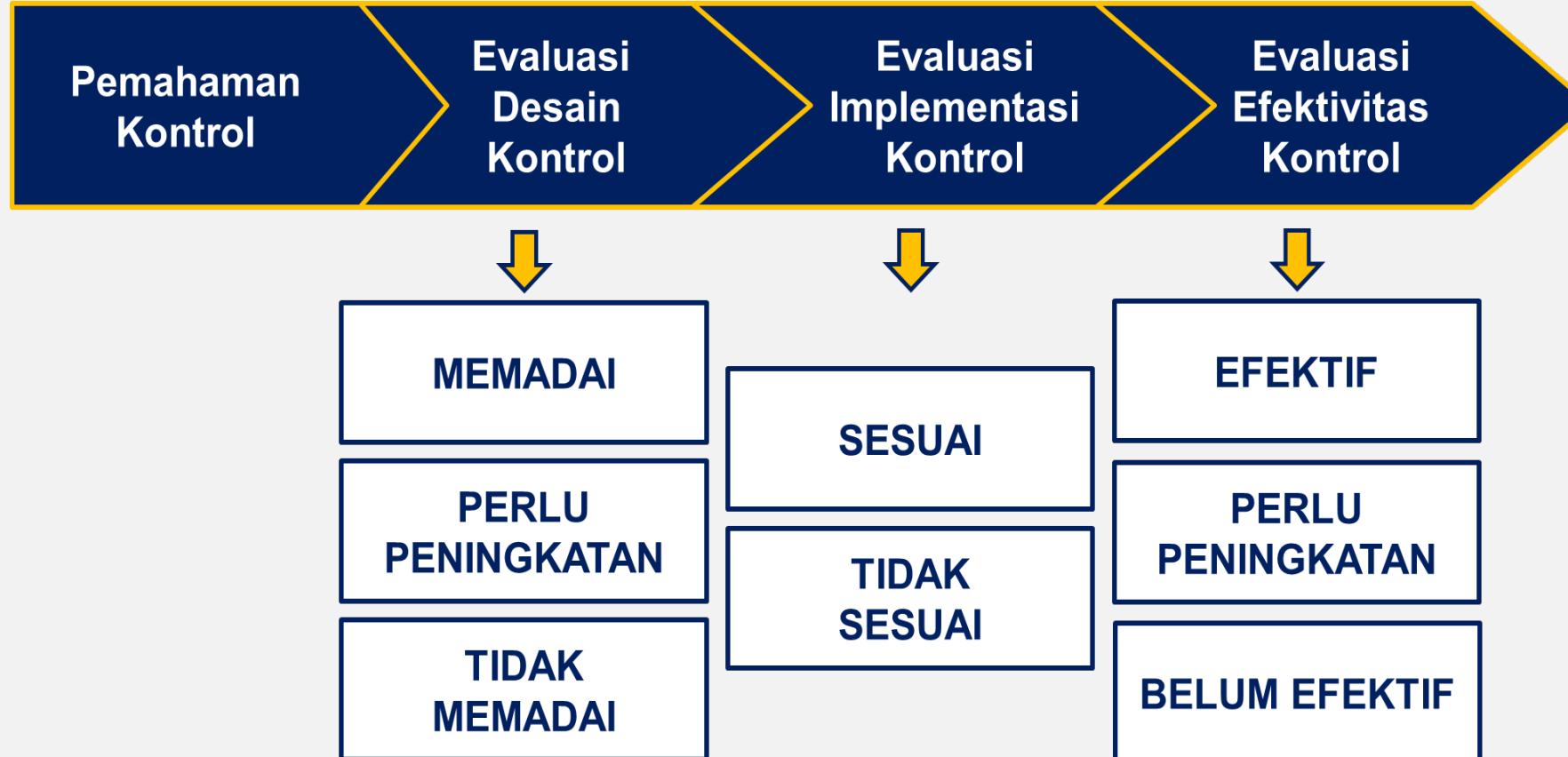
EFEKTIF

PERLU PENINGKATAN

TIDAK EFEKTIF



KESIMPULAN AUDIT KEAMANAN SPBE



METODE PENARIKAN KESIMPULAN

Desain Kontrol (nasional)	Kondisi	Evaluasi Desain Kontrol aplikasi/infra)	Evaluasi Implementasi Kontrol	Evaluasi Efektivitas Kontrol	Konklusi Audit
Perban 4	1	Memadai	Sesuai Dengan Desain Kontrol	Efektif	Memadai
				Perlu Peningkatan	Memadai
				Belum Efektif	Perlu Peningkatan
	2	Perlu Peningkatan	Tidak Sesuai Dengan Desain Kontrol	Efektif	Perlu Peningkatan
				Perlu Peningkatan	Tidak Memadai
				Belum Efektif	Tidak Memadai
	3	Tidak Memadai	Sesuai Dengan Desain Kontrol	Efektif	Memadai
				Perlu Peningkatan	Perlu Peningkatan
				Belum Efektif	Tidak Memadai
			Tidak Sesuai Dengan Desain Kontrol	Efektif	Tidak Memadai
				Perlu Peningkatan	Tidak Memadai
				Belum Efektif	Tidak Memadai

TAHAP PELAPORAN

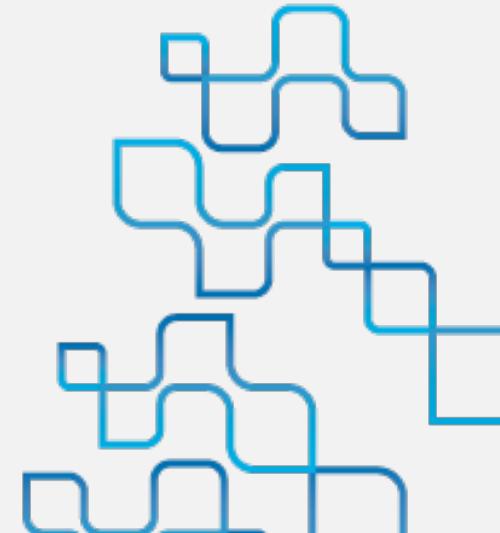
TUJUAN TAHAP PELAPORAN



Tujuan Tim Auditor melaksanakan kegiatan ini adalah untuk melakukan penyusunan Laporan Hasil Audit Keamanan (LHAK), termasuk di dalamnya dokumen Rencana Tindak Lanjut atas temuan hasil pelaksanaan Audit Keamanan Aplikasi Khusus yang komprehensif dan terukur dalam melaksanakan Audit Keamanan.



KEGIATAN TAHAP PELAPORAN



TAHAP EVALUASI

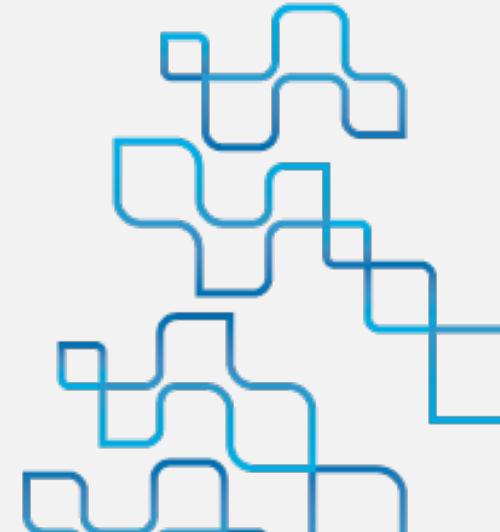


TUJUAN TAHAP EVALUASI

Tujuan Tim Auditor melaksanakan kegiatan ini adalah untuk melakukan pemantauan, evaluasi, serta verifikasi terhadap tindak lanjut atas temuan dan rekomendasi Audit Keamanan.



KEGIATAN TAHAP EVALUASI



NEXT OUTLINE MATERI

KRITERIA DAN KONTROL KEAMANAN



KRITERIA

Kriteria yaitu berbagai peraturan perundang-perundangan dan/atau kebijakan, prosedur, dan instruksi kerja, serta standar dan praktik-praktik terbaik, yang digunakan oleh Auditor TIK untuk melakukan evaluasi dan pengujian atas pengendalian intern TIK, manajemen risiko TIK dan tata kelola TIK

(Peraturan Menteri Kominfo 16/2022)



KONTROL KEAMANAN

Sekumpulan aktivitas keamanan yang harus didefinisikan dan dilaksanakan. Kontrol keamanan diturunkan dari kriteria audit keamanan.



KESEPAKATAN SEMENTARA KRITERIA AUDIT KEAMANAN SPBE (Lingkup Amanat Perpres 95/2018)

- 1. PELAKSANAAN MANAJEMEN KEAMANAN SPBE DAN**
- 2. PENERAPAN KEAMANAN SPBE BERDASARKAN STANDAR TEKNIS KEAMANAN SPBE**

MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 48 ayat 4: IPPD melaksanakan
MKI SPBE

Pasal 48 ayat 5: Pedoman Manajemen keamanan Infromasi
SPBE diatur oleh BSSN

STANDAR TEKNIS DAN PROSEDUR TEKNIS :

- ✓ Pasal 41 ayat 3: Penerapan Keamanan harus memenuhi Standar Teknis & Prosedur Keamanan SPBE
- ✓ Pasal 41 ayat 4: Ketentuan Standar Teknis & Prosedur Keamanan diatur oleh BSSN

**PERATURAN BSSN No. 4 tahun 2021
tentang Pedoman SMKI SPBE dan Standar
Teknis dan Prosedur Keamanan SPBE**

NEXT OUTLINE MATERI



PROSEDUR PADA TAHAPAN PELAKSANAAN AUDIT KEAMANAN SPBE



BADAN SIBER
DAN SANDI
NEGARA

Pemahaman
Desain Kontrol

Evaluasi
Implementasi
Kontrol

1

2

3

4

Evaluasi Desain
Kontrol

Evaluasi
Efektivitas
Kontrol



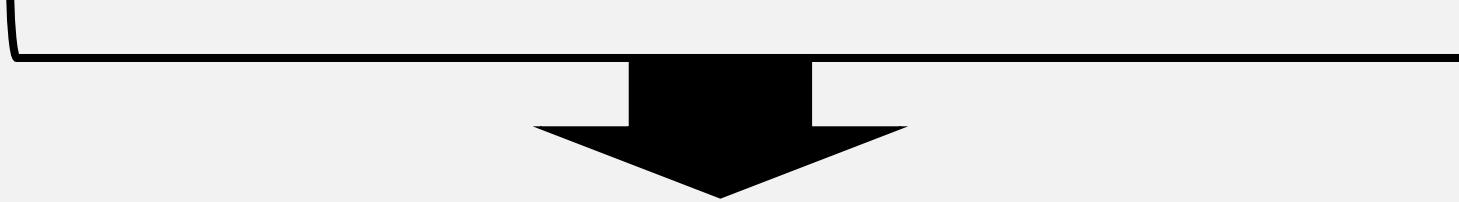
DESAIN INSTRUMEN

Pemeriksaan Hal Pokok Teknis

1. Tata Kelola Keamanan SPBE.
2. Manajemen Keamanan Informasi SPBE.
3. Fungsionalitas dan Kinerja.
4. Aspek Keamanan TIK Lainnya

Kriteria Audit Keamanan

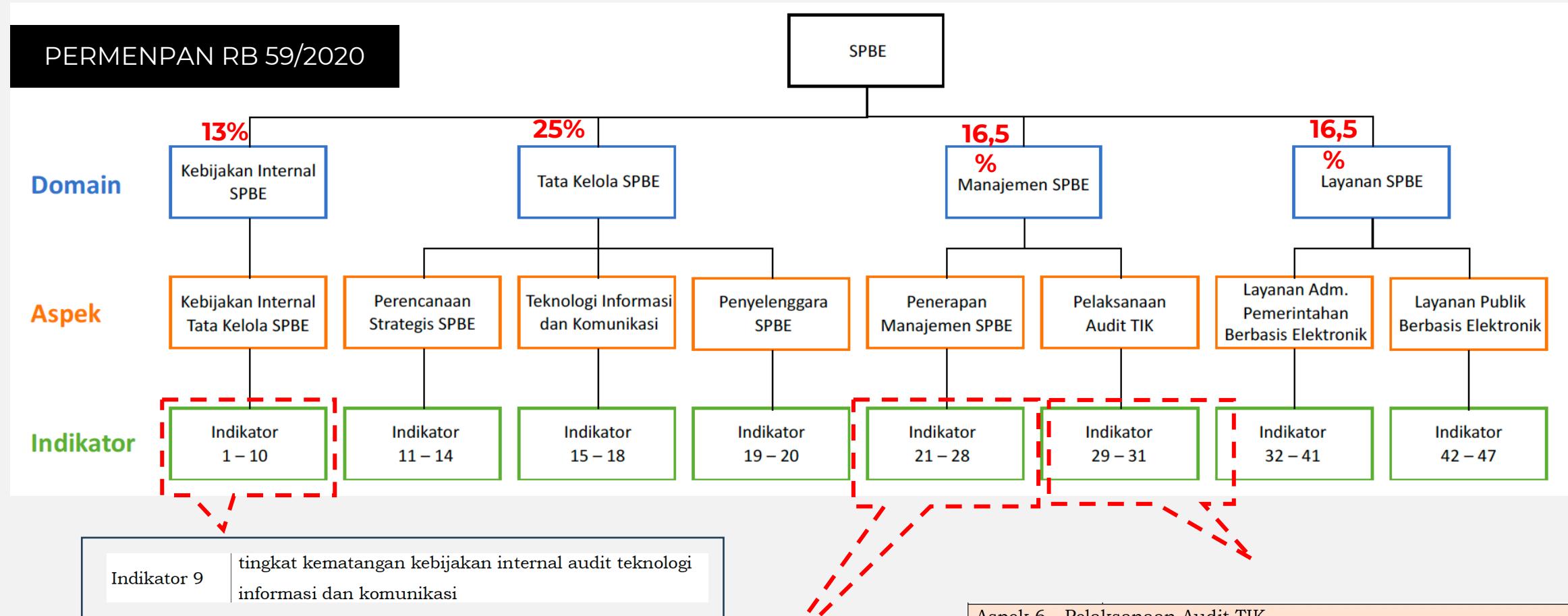
1. Kebijakan Keamanan Makro
2. Kebijakan Keamanan Meso
3. Kebijakan Keamanan Mikro



**Audit Tools/
Instrumen Audit Keamanan SPBE**



INDEKS SPBE CAPAIAN KEBIJAKAN DAN PELAKSANAAN AUDIT KEAMANAN SPBE



INDIKATOR 8

Tingkat Kematangan Kebijakan Internal Manajemen Keamanan Informasi

INDIKATOR 22

Tingkat Kematangan Penerapan Manajemen Keamanan SPBE

Aspek 6 - Pelaksanaan Audit TIK

Indikator 29	Tingkat Kematangan Pelaksanaan Audit Infrastruktur SPBE
Indikator 30	Tingkat Kematangan Pelaksanaan Audit Aplikasi SPBE
Indikator 31	Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

AUDIT KEAMANAN SPBE

INDIKATOR 31 : Tingkat Kematangan Pelaksanaan Audit

Keamanan SPBE

TINGKAT 5:

Kriteria tingkat 4 telah terpenuhi dan hasil audit Keamanan SPBE telah ditindaklanjuti melalui perbaikan penerapan Keamanan SPBE.

TINGKAT 4:

Kriteria tingkat 3 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan oleh auditor TIK/Sistem Keamanan Informasi eksternal yang memiliki sertifikasi auditor TIK/Sistem Keamanan Informasi.

TINGKAT 3:

Kriteria tingkat 2 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan pedoman Audit Keamanan. Kondisi : kegiatan Audit Keamanan dilaksanakan oleh auditor TIK/Sistem Keamanan Informasi internal Instansi Pusat/Pemerintah Daerah.

TINGKAT 2:

Kriteria tingkat 1 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan perencanaan berkesinambungan. Kondisi : Kegiatan Audit Keamanan dilaksanakan tanpa pedoman Audit Keamanan.

TINGKAT 1:

Kegiatan Audit Keamanan SPBE belum atau telah dilaksanakan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa perencanaan yang berkesinambungan

DOMAIN 3 : MANAJEMEN SPBE

ASPEK 6 : PELAKSANAAN AUDIT TIK



Terima Kasih

