BADAN SIBER DAN SANDI NEGARA

AUDIT KEAMANAN SPBE

Disampaikan pada Sosialisasi dan Asistensi terkait Kebijakan Tata Kelola TIK dalam Mendukung Penyelenggaraan SPBE, SDI, Transformasi Digital dan Keterpaduan Layanan Digital di Pemerintah

- Direktorat Keamanan Siber dan Sandi Pemerintah Daerah -
Diah Sulistyowati

Palangka Raya, 27 Juni 2024

TLP:CLEAR

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten
Harmonis Loyal Adaptif Kolaboratif

Agenda

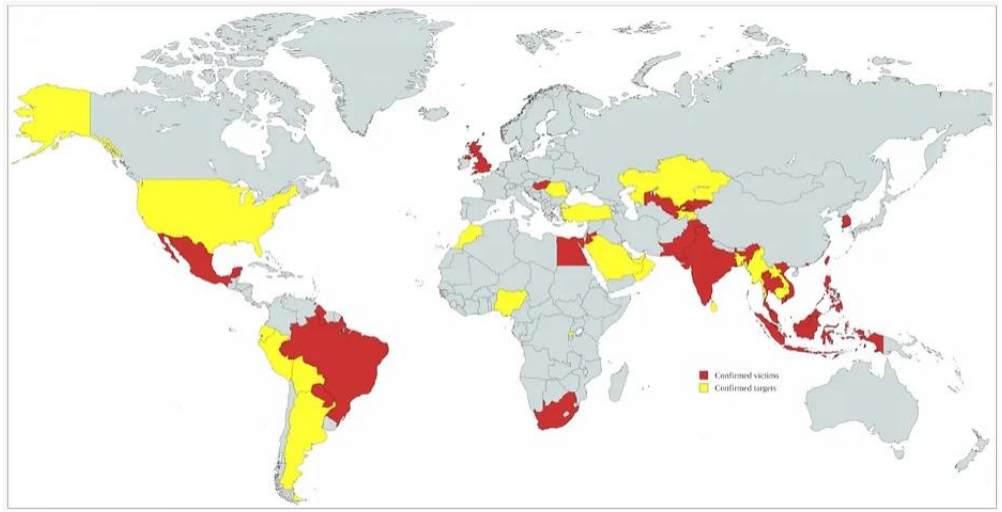
Audit Keamanan SPBE

1. Tantangan Keamanan SPBE
2. Pengaturan Audit Keamanan SPBE
3. Pelaksanaan Audit Keamanan SPBE
4. Peran Audit Internal Keamanan SPBE
5. Kesimpulan

BADAN SIBER DAN SANDI NEGARA

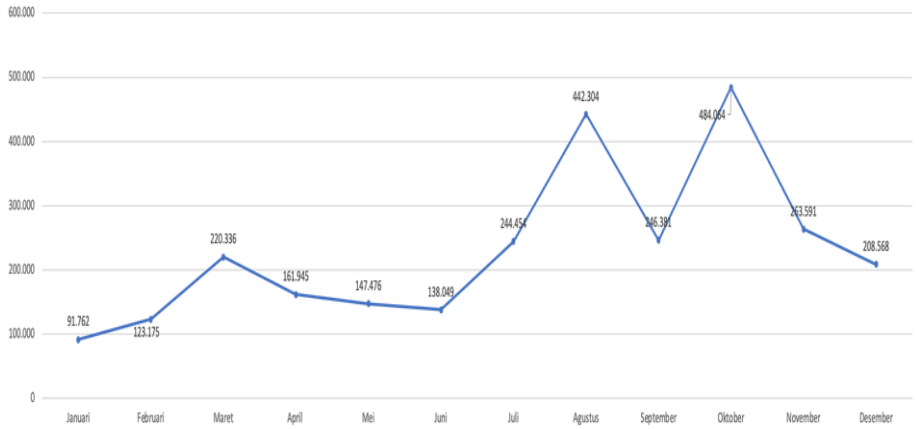
TANTANGAN KEAMANAN SPBE

Serangan Hacker Earth Krahang



ref: www.trendmicro.com

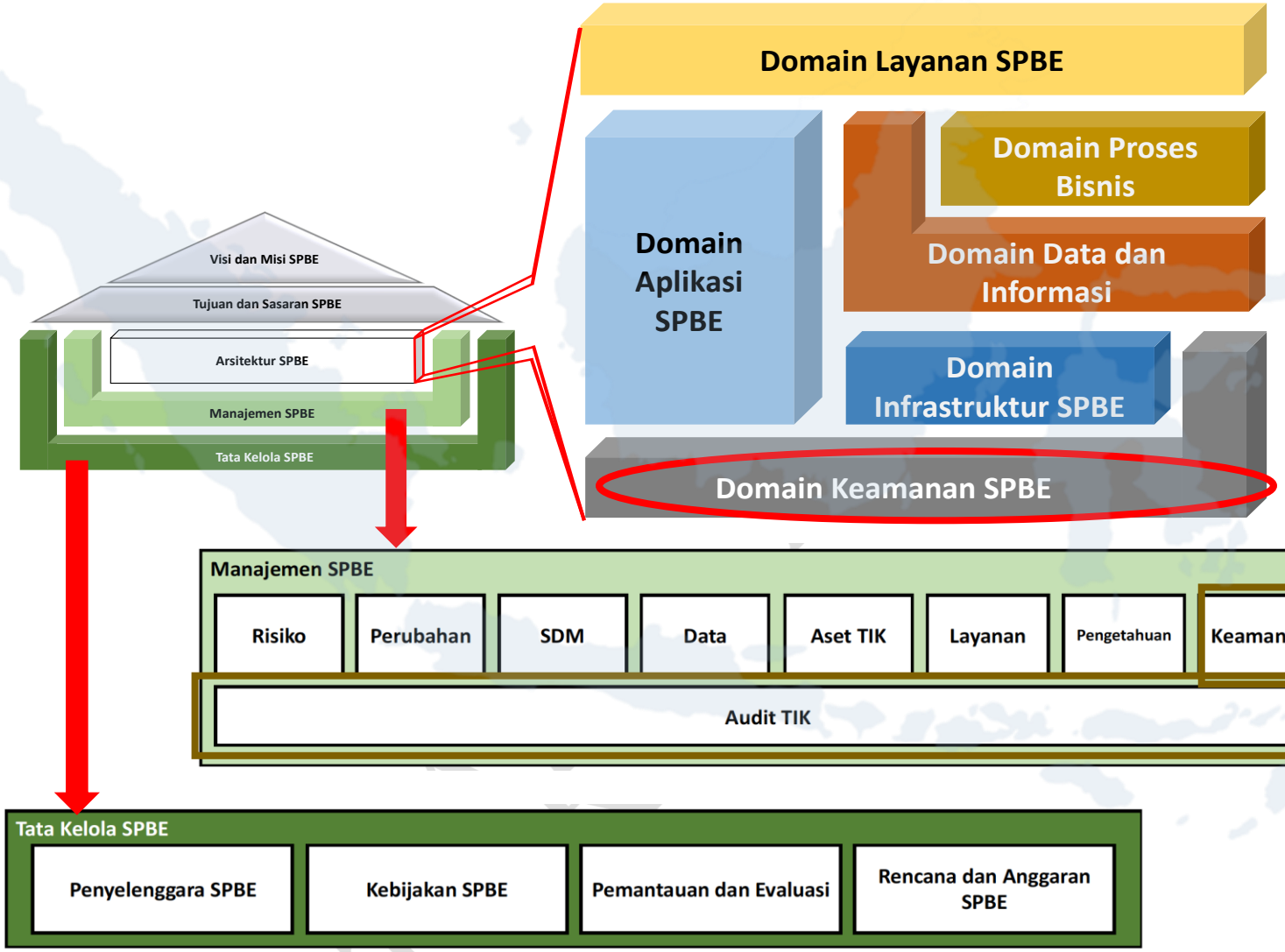
Anomali Trafik Keamanan Siber di Pemerintah Daerah TA2023



ref: Landskap Keamanan Siber 2023

BADAN SIBER DAN SANDI NEGARA

KERANGKA KERJA ARSITEKTUR SPBE



Perpres No. 95 Tahun 2018

Pasal 48

(1) Manajemen keamanan informasi sebagaimana dimaksud dalam Pasal 46 ayat (1) huruf b bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi.

(2) Manajemen keamanan informasi dilakukan melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE.

(3) Manajemen keamanan informasi sebagaimana dimaksud pada ayat (2) dilaksanakan berdasarkan pedoman manajemen keamanan informasi SPBE.

(4) Dalam pelaksanaan manajemen keamanan informasi, pimpinan Instansi Pusat dan kepala daerah berkoordinasi dan dapat melakukan konsultasi dengan kepala lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

(5) Ketentuan lebih lanjut mengenai pedoman manajemen keamanan informasi SPBE diatur dengan Peraturan Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

KEBIJAKAN
Sistem Manajemen Keamanan Informasi
(Perban BSSN No. 4 Tahun 2021)

AUDIT TIK
(termasuk di dalamnya audit TIK)
❑ Permenkominfo No. 16 Tahun 2022 (KUPATIK)
❑ Rancangan Peraturan BSSN (teknis)

MANDATORY INSTANSI PEMERINTAH TERHADAP KEAMANAN SPBE

REGULASI KEAMANAN SPBE

01 **UU No.27 Tahun 2022** tentang Pelindungan Data Pribadi (PDP)

02 **UU No.1 Tahun 2024** tentang Informasi Transaksi Elektronik (ITE)

03 **Perpres 95 Tahun 2018** tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)

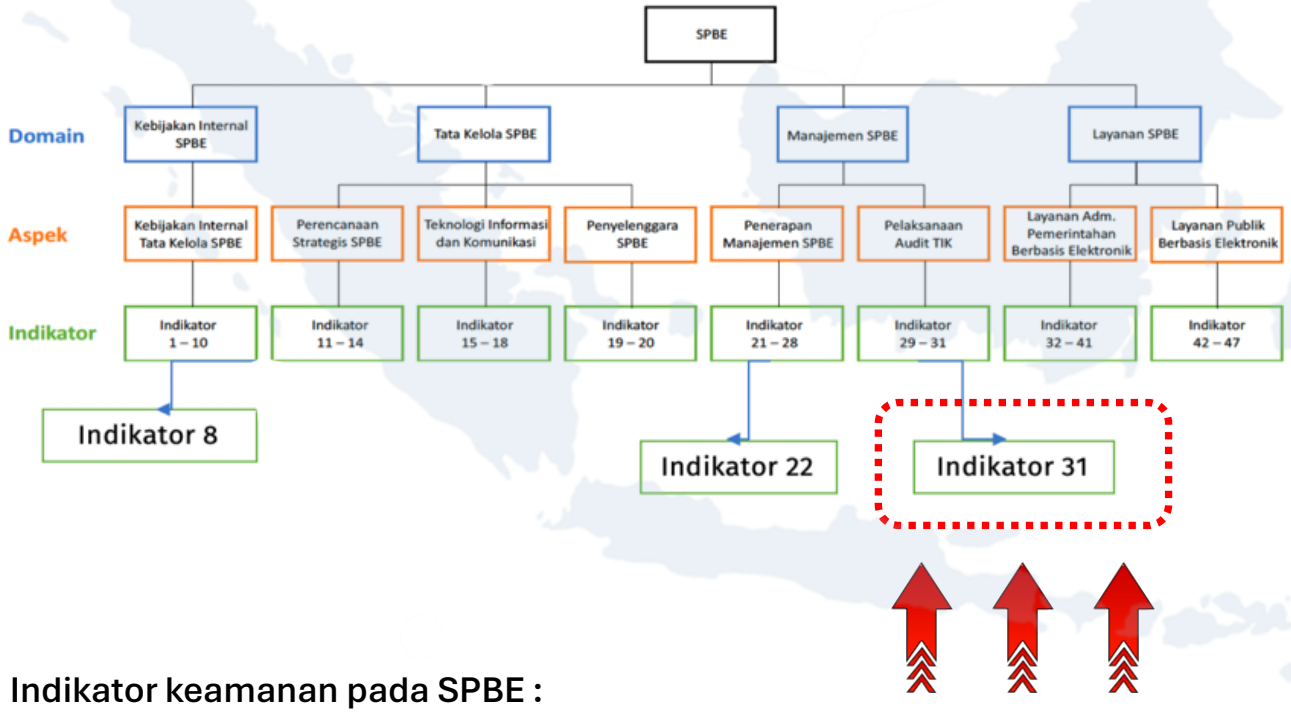
04 **Perpres 82 Tahun 2022** tentang Pelindungan Infrastruktur Informasi Vital (PIIV)

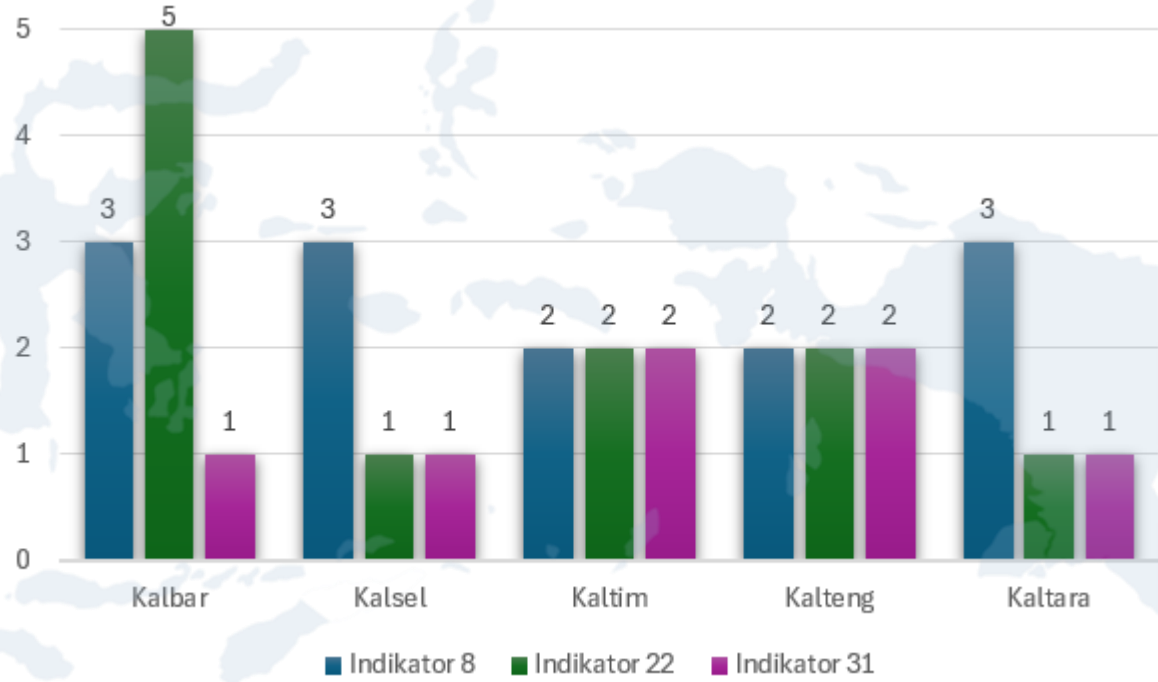
05 **Perpres 47 Tahun 2023** tentang Strategi Keamanan Siber Nasional (SKSN) dan Manajemen Kriisis Siber Nasional (MKS)

- **Kewajiban penerapan Keamanan SPBE [Pasal 41]**
- **Melaksanakan Manajemen Keamanan Informasi [Pasal 48]**
- **Audit Keamanan SPBE [Pasal 58]**

BADAN SIBER DAN SANDI NEGARA

Struktur Penilaian Tingkat Kematangan SPBE sesuai Permenpan 59 tahun 2020 dan Hasil Pemantauan dan Evaluasi TA2023





Indikator keamanan pada SPBE :

- Indikator 8 : Tingkat Kematangan Kebijakan Internal Manajemen Keamanan Informasi
- Indikator 22 : Tingkat Kematangan Penerapan Manajemen Keamanan Informasi
- Indikator 31 : Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

BADAN SIBER DAN SANDI NEGARA

TINGKAT KEMATANGAN AUDIT KEAMANAN SPBE

Indikator 31 : Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE
Pertanyaan : Apakah Instansi Pusat/Pemerintah Daerah melaksanakan Audit Keamanan SPBE?

Tingkat	Kriteria
1	Kegiatan Audit Keamanan SPBE belum atau telah dilaksanakan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa perencanaan yang berkesinambungan.
2	Kriteria tingkat 1 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan perencanaan yang berkesinambungan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa pedoman Audit Keamanan.
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.
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.
5	Kriteria tingkat 4 telah terpenuhi dan hasil audit Keamanan SPBE telah ditindaklanjuti melalui perbaikan penerapan Keamanan SPBE.

01 Belum dilaksanakan atau dilaksanakan tanpa perencanaan

02 Telah dilaksanakan sesuai perencanaan tanpa pedoman audit keamanan

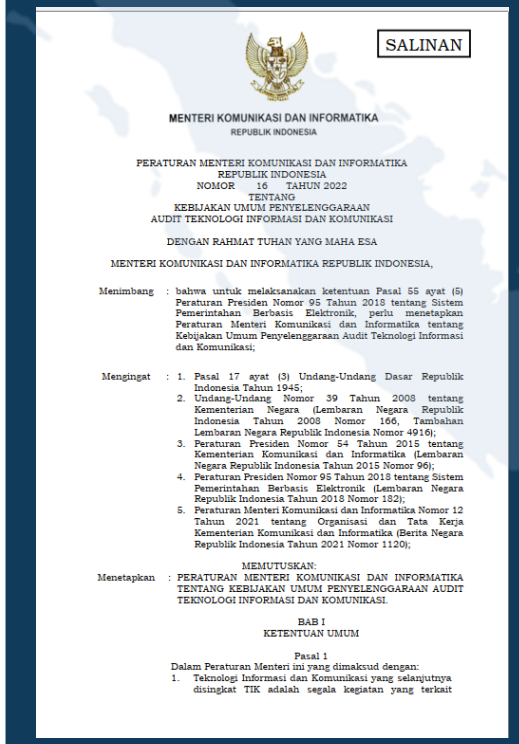
03 Audit internal telah dilaksanakan sesuai perencanaan dengan pedoman audit keamanan

04 Audit eksternal telah dilaksanakan sesuai perencanaan sesuai pedoman audit keamanan

05 Perbaikan berkelanjutan

BADAN SIBER DAN SANDI NEGARA

Delegasi Tugas Aparat Pengawasan Intern Pemerintah (APIP) pada Audit TIK Internal



SALINAN

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA
NOMOR 16 TAHUN 2022
TENTANG
KEBIJAKAN UMUM PENYELENGGARAAN
AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 55 ayat (5) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Menteri Komunikasi dan Informatika tentang Kebijakan Umum Penyelenggaraan Audit Teknologi Informasi dan Komunikasi;

Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);
3. Peraturan Presiden Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 96);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
5. Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika (Berita Negara Republik Indonesia Tahun 2021 Nomor 1120);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA TENTANG KEBIJAKAN UMUM PENYELENGGARAAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:
1. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait

PERMENKOMINFO NO 16 TAHUN 2022 TENTANG KEBIJAKAN UMUM PENYELENGGARAAN AUDIT TIK

Pasal 17

(1) Selain Lembaga Pelaksana Audit TIK pemerintah atau Lembaga Pelaksana Audit TIK Terakreditasi, untuk kebutuhan internal Instansi Pusat dan Pemerintah Daerah, unit kerja Instansi Pusat dan Pemerintah Daerah yang memiliki fungsi pengawasan internal melaksanakan audit TIK internal secara periodik.

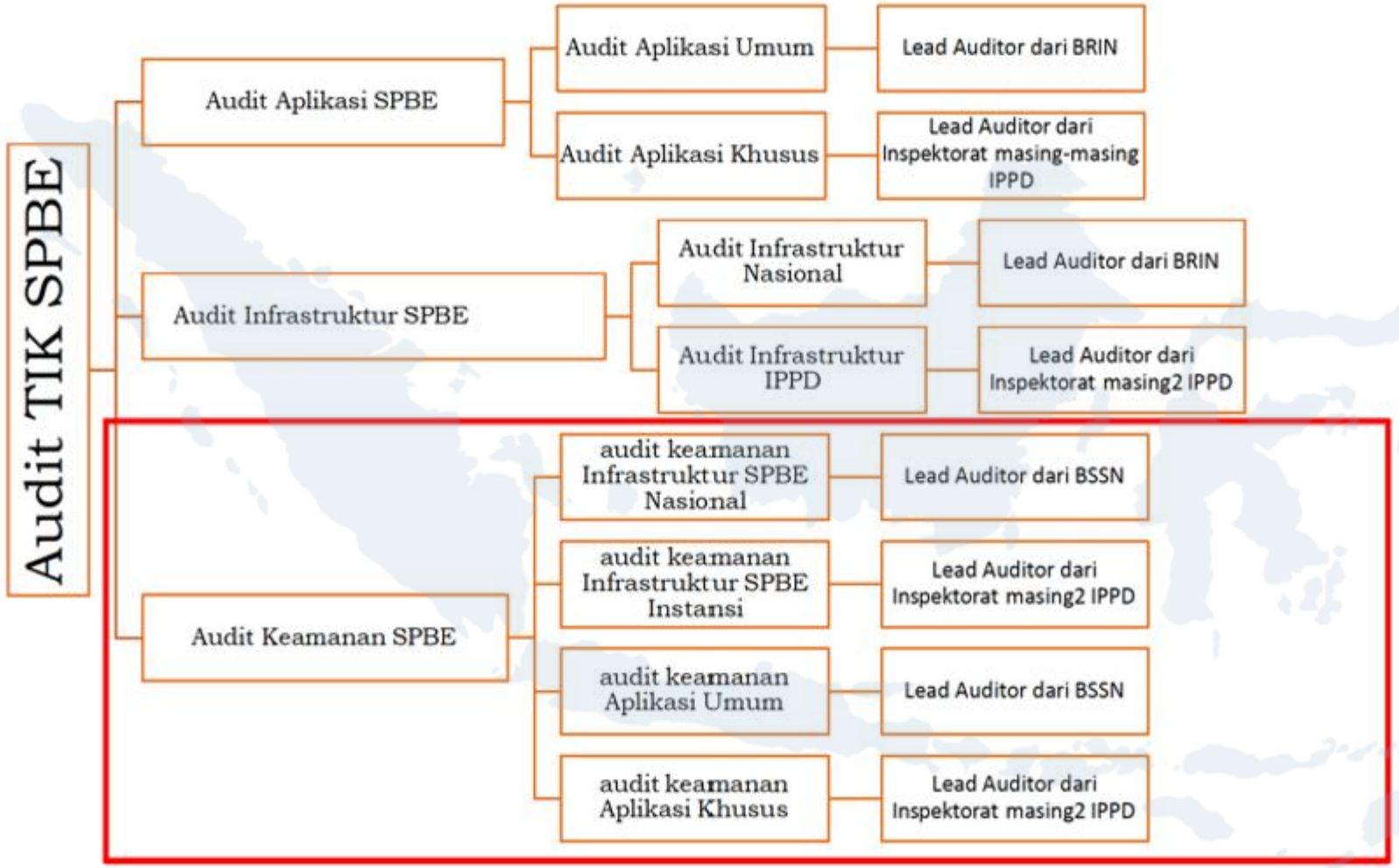
(2) Pelaksanaan audit TIK internal sebagaimana dimaksud pada ayat (1) mengacu pada kebijakan Audit TIK.

(3) Pelaksanaan audit TIK internal sebagaimana dimaksud pada ayat (1), dapat melibatkan pegawai Aparatur Sipil Negara dari unit kerja lain yang memiliki kompetensi Audit TIK.

(4) Pelaksanaan audit TIK internal oleh unit kerja sebagaimana dimaksud pada ayat (1) tidak menghilangkan kewajiban Audit TIK oleh Lembaga Pelaksana Audit TIK pemerintah atau Lembaga Pelaksana Audit TIK Terakreditasi.

BADAN SIBER DAN SANDI NEGARA

TOPOLOGI/AUDIT SEGMENTASI AUDIT TIK SPBE (PERPRES 95/2018)



Pasal 58 ayat 2:

dilaksanakan berdasarkan standar dan tata cara pelaksanaan audit Keamanan SPBE

Pasal 58 ayat 3:

Audit keamanan Infrastruktur SPBE Nasional dan Aplikasi Umum dilaksanakan 1 (satu) kali dalam 1 (satu) tahun oleh BSSN

Pasal 58 ayat 4:

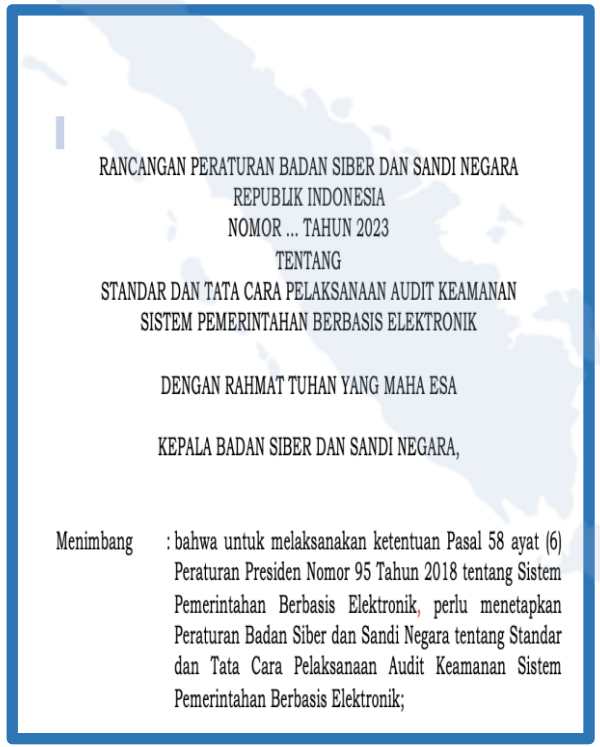
Audit keamanan Infrastruktur SPBE IPPD dan Aplikasi khusus dilakukan paling sedikit 1 (satu) kali dalam 2 (dua) tahun oleh IPPD

KETERANGAN:

- Pada Pelaksanaan Audit Internal, Lead Auditor dari Inspektorat masing-masing IPPD dapat melibatkan ASN dari unit kerja lain yang memiliki kompetensi audit TIK.
- Pada Pelaksanaan Audit Eksternal, IPPD melaksanakan Audit TIK dengan menunjuk LATIK Terakreditasi dan Terdaftar, apabila belum ada maka dilakukan oleh LATIK Pemerintah.

BADAN SIBER DAN SANDI NEGARA

PENGATURAN AUDIT KEAMANAN SPBE (RPBSSN STA)



RANCANGAN PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR ... TAHUN 2023
TENTANG
STANDAR DAN TATA CARA PELAKSANAAN AUDIT KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 58 ayat (6) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik;

RUANG LINGKUP RPBSSN STA

Standar Audit Keamanan SPBE

a. objek Audit Keamanan SPBE;
b. pelaksana Audit Keamanan SPBE;
c. kriteria Audit Keamanan SPBE;
d. bukti Audit Keamanan SPBE; dan
e. kesimpulan Audit Kemanan SPBE.

Tata cara pelaksanaan Audit Keamanan SPBE

a. Tata cara umum pelaksanaan Audit Keamanan SPBE;
b. Tata cara pelaporan Audit Keamanan SPBE;
c. Tata cara tindak lanjut Audit Keamanan SPBE;
d. Tata cara pendaftaran pelaksana Audit Keamanan SPBE; dan
e. Tata cara pengalokasian sumber daya.

Pembiayaan Audit Keamanan SPBE

a. sumber pembiayaan;
b. tanggung jawab perencanaan dan penganggaran;
c. mekanisme penunjukan; dan
d. besaran biaya.

BADAN SIBER DAN SANDI NEGARA

KRITERIA AUDIT KEAMANAN SPBE

DEFINISI KRITERIA

Kriteria yaitu berbagi 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 TIL, maanjemen risiko TIK dan taat kelola TIK (Peraturan Menteri Kominfo 16/2022)

Auditor yang melaksanakan audit keamanan untuk kebutuhan internal menggunakan kriteria Audit Keamanan SPBE yang disepakati oleh APIP

KRITERIA*

1. kebijakan **makro** terkait Keamanan SPBE dan pelindungan privasi (berupa undang-undang yang mengatur lebih luas kepentingan Masyarakat, pelaku usaha dan pihak-pihak terkait)
2. kebijakan **meso** terkait Keamanan SPBE dan pelindungan privasi (yang menjelaskan suatu pengaturan berupa peraturan menteri dan peraturan badan yang berlaku bagi semua Instansi Pusat dan Pemerintah Daerah)
3. kebijakan **mikro** terkait Keamanan SPBE dan pelindungan privasi (kebijakan internal Instansi Pusat dan Pemerintah Daerah terkait)

**) ditetapkan Kepala BSSN*

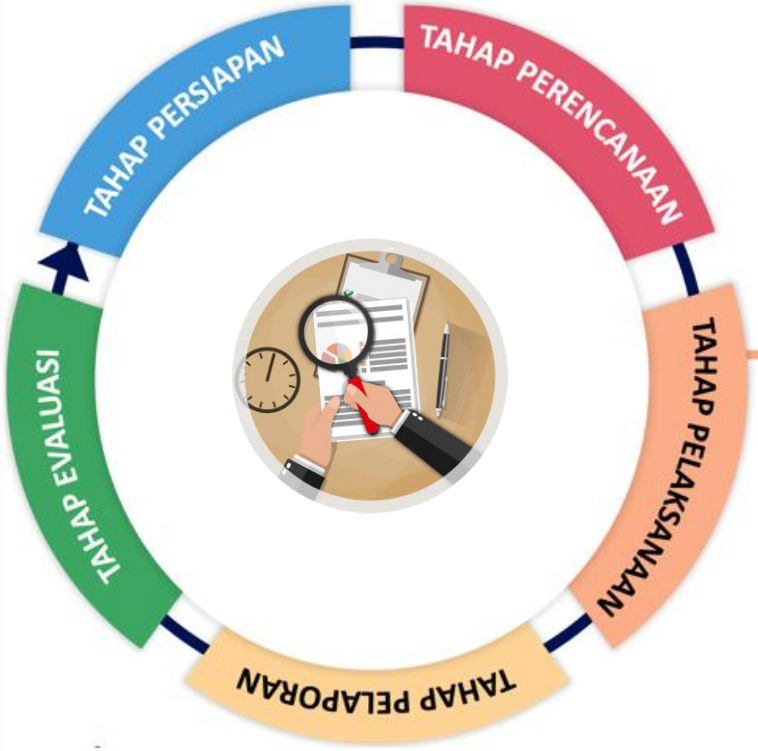
Kebijakan yang akan menjadi kriteria Audit Keamanan SPBE ditetapkan oleh Kepala BSSN, didalamnya antara lain **Peraturan BSSN 4/2021**

BADAN SIBER DAN SANDI NEGARA

PROSES AUDIT KEAMANAN APLIKASI UMUM & INFRASTRUKTUR SPBE NASIONAL

AREA AUDIT KEAMANAN SPBE

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



- EVALUASI DESAIN KONTROL
- EVALUASI IMPLEMENTASI KONTROL
- EVALUASI EFEKTIVITAS KONTROL

- **Peraturan BSSN No 4 Tahun 2021** tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE

Pada RPB STA terbaru, tata cara pelaksanaan audit keamanan untuk internal dapat menggunakan tata cara pelaksanaan audit yang sudah ada (pedoman pelaksanaan audit di unit pengawasan masing-masing). Tata cara ini berlaku untuk lembaga pelaksana audit TIK terakreditasi cakupan keamanan

BADAN SIBER DAN SANDI NEGARA

KEBUTUHAN DOKUMEN AWAL AUDIT KEAMANAN APLIKASI /INFRASTRUKTUR SPBE

1. Surat perintah/tugas tim auditan 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 yang akan di audit;
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 yang di audit;
7. Dokumen yang memuat analisis risiko terkait dengan aplikasi dan pendukungnya.

BADAN SIBER DAN SANDI NEGARA

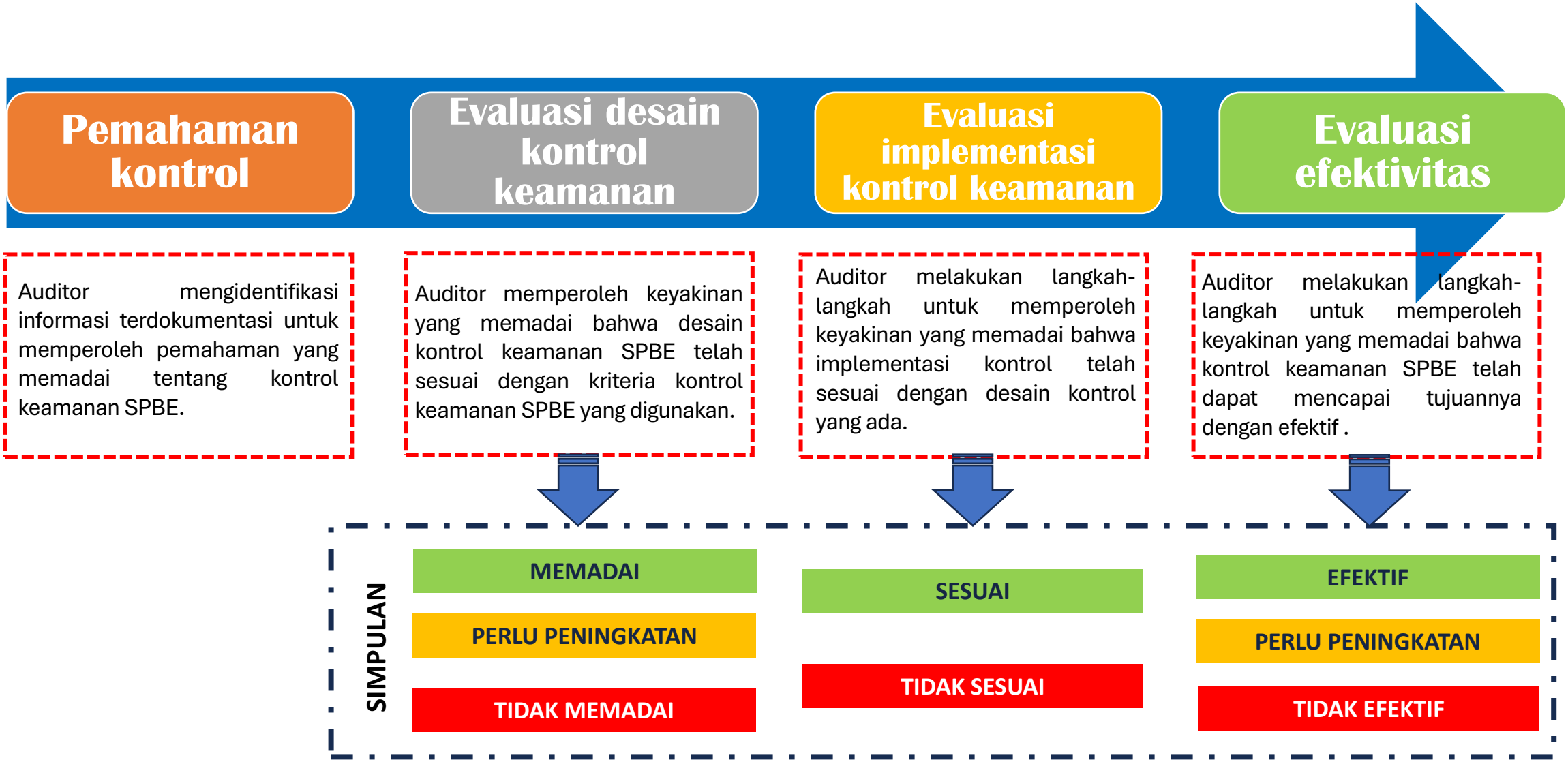
TAHAP PELAKSANAAN AUDIT KEAMANAN SPBE

Tujuan:

1. **Memperoleh KESIMPULAN dari setiap Tahapan Audit yang dilaksanakan.**
2. **KESIMPULAN berupa kesesuaian objek yang diaudit dibandingkan dengan KRITERIA AUDIT dan TEMUAN hasil pelaksanaan objek audit**

BADAN SIBER DAN SANDI NEGARA

PROSEDUR AUDIT KEAMANAN APLIKASI UMUM BIDANG ABC



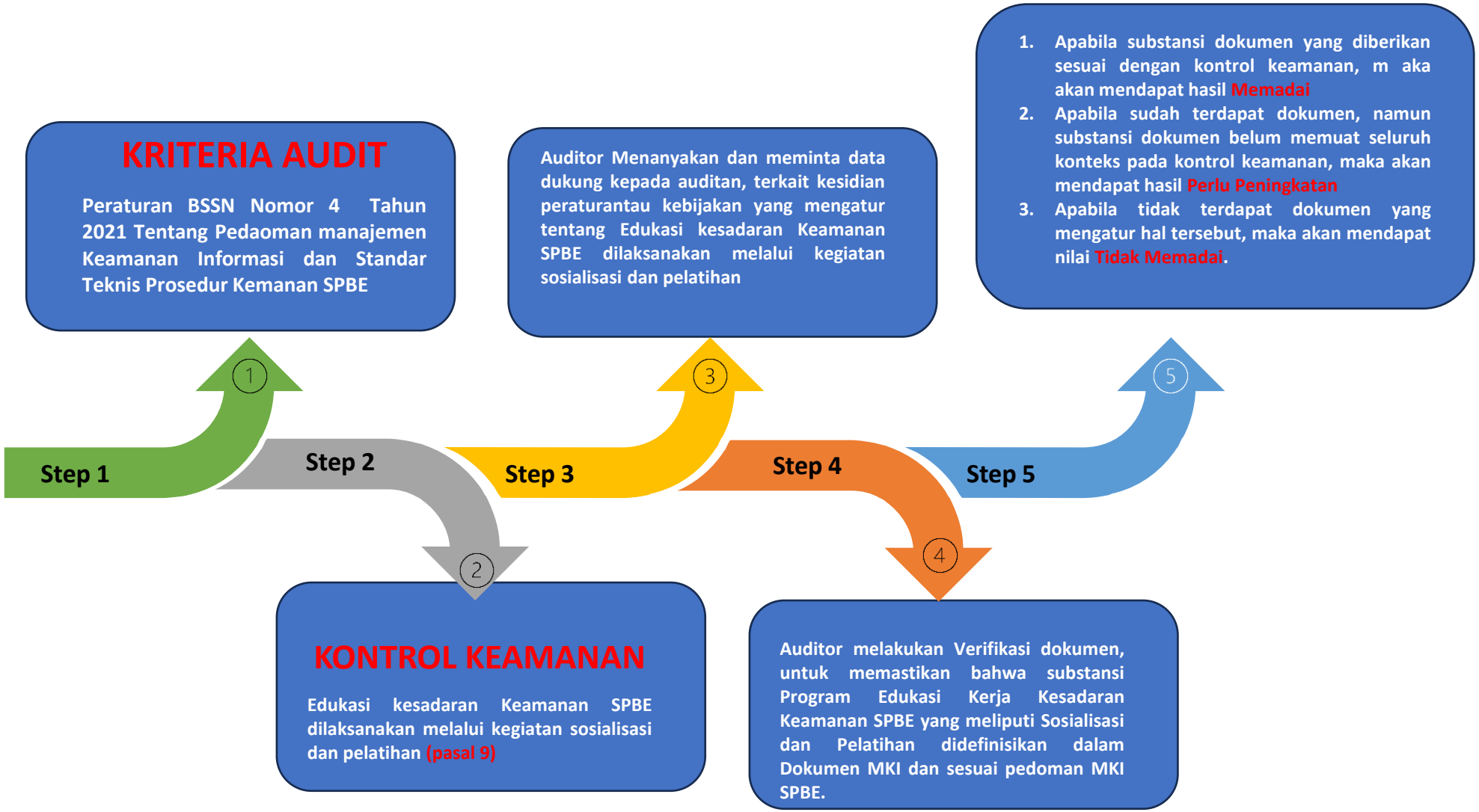
BADAN SIBER DAN SANDI NEGARA

MATRIKS KESIMPULAN AUDIT KEAMANAN SPBE

Hasil Evaluasi Desain Pengendalian	Hasil Evaluasi Implementasi Pengendalian	Hasil Pengujian Terinci Efektivitas Pengendalian	Kesimpulan Audit Keamanan SPBE
Memadai	Sesuai Dengan Desain Pengendalian	Efektif	Memadai
		Perlu Peningkatan	Memadai
		Belum Efektif	Perlu Peningkatan
	Tidak Sesuai Dengan Desain Pengendalian	Efektif	Perlu Peningkatan
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai
Perlu Peningkatan	Sesuai Dengan Desain Pengendalian	Efektif	Memadai
		Perlu Peningkatan	Perlu Peningkatan
		Belum Efektif	Tidak Memadai
	Tidak Sesuai Dengan Desain Pengendalian	Efektif	Tidak Memadai
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai
Tidak Memadai	-	Efektif	Tidak Memadai
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai

BADAN SIBER DAN SANDI NEGARA

CONTOH: EVALUASI DESAIN KONTROL AREA MANAJEMEN KI



CONTOH: EVALUASI IMPLEMENTASI KONTROL AREA MANAJEMEN KI

KRITERIA AUDIT

Peraturan BSSN Nomor 4 Tahun 2021 Tentang Pedaoman manajemen Keamanan Informasi dan Standar Teknis Prosedur Kemanan SPBE

Step 1

Step 2

KONTROL KEAMANAN

Edukasi kesadaran Keamanan SPBE dilaksanakan melalui kegiatan sosialisasi dan pelatihan (pasal 9)

Step 3

Auditor melakukan Wawancara dan verifikasi bukti dokumen yang diberikan Auditan, untuk memastikan berjalannya kegiatan edukasi kesadaran keamanan berupa sosialisasi dan pelatihan.

Step 4

1. Apabila desain kontrol keamanan dilaksanakan dan t erdapat bukti dukung yang memadai, maka akan me ndapat nilai Sesuai Desain Kontrol;
2. Apabila desain kontrol keamanan tidak dilaksanakan , maka akan mendapat nilai Tidak Sesuai Desain.

BADAN SIBER DAN SANDI NEGARA

CONTOH: EVALUASI EFEKTIVITAS KONTROL AREA MANAJEMEN KI

1

Kriteria Audit

Peraturan BSSN Nomor 4 Tahun 2021 Tentang Pedaoman manajemen Keamanan Informasi dan Standar Teknis Prosedur Kemanan SPBE

2

Kontrol Keamanan

Edukasi kesadaran Keamanan SPBE dilaksanakan melalui kegiatan sosialisasi dan pelatihan (pasal 9)

3

Auditor melakukan Pemeriksaan substansial untuk memastikan tujuan peningkatan pengetahuan kesadaran keamanan SPBE telah terpenuhi melalui sosialisasi dan pelatihan untuk internal Organisasi dan pihak eksternal terkait.

1. Pemeriksaan dilakukan dengan metode Survei (uji sampling) terhadap personel Internal Organisasi dan pihak eksternal dilakukan.
2. Personel yang menjadi subjek sampling adalah yang hadir dalam kegiatan sosialisasi dan atau pelatihan keamanan SPBE.\
3. Penggunaan metode uji sampling disampaikan kepada auditan, dan melihat kondisi dan waktu yang tersedia.

4

1. Apabila tidak ada risiko yang terbukti terjadi dari implementasi keamanan, maka akan mendapat nilai Efektif
2. Apabila terdapat sedikit kekurangan dan tidak menimbulkan risiko dari implementasi keamanan yang telah dilakukan, maka akan mendapat nilai Perlu Peningkatan
3. Apabila ada risiko yang terbukti terjadi dari implementasi keamanan, maka akan mendapat nilai Belum Efektif

CONTOH: EVALUASI DESAIN KONTROL AREA STANDAR TEKNIS

1

Kriteria Audit:
Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE

3

Auditor menanyakan kepada Auditan terkait ketersediaan peraturan atau kebijakan yang mengatur tentang pengaturan kata sandi pada objek audit.

5

1. Apabila substansi dokumen yang diberikan sesuai dengan kontrol keamanan, maka akan mendapat hasil **Memadai**
2. Apabila sudah terdapat dokumen, namun substansi dokumen belum memuat seluruh konteks pada kontrol keamanan, maka akan mendapat hasil **Perlu Peningkatan**
3. Apabila tidak terdapat dokumen yang mengatur hal tersebut, maka akan mendapat nilai **Tidak Sesuai**

Step 1 → Step 2 → Step 3 → Step 4 → Step 5

2

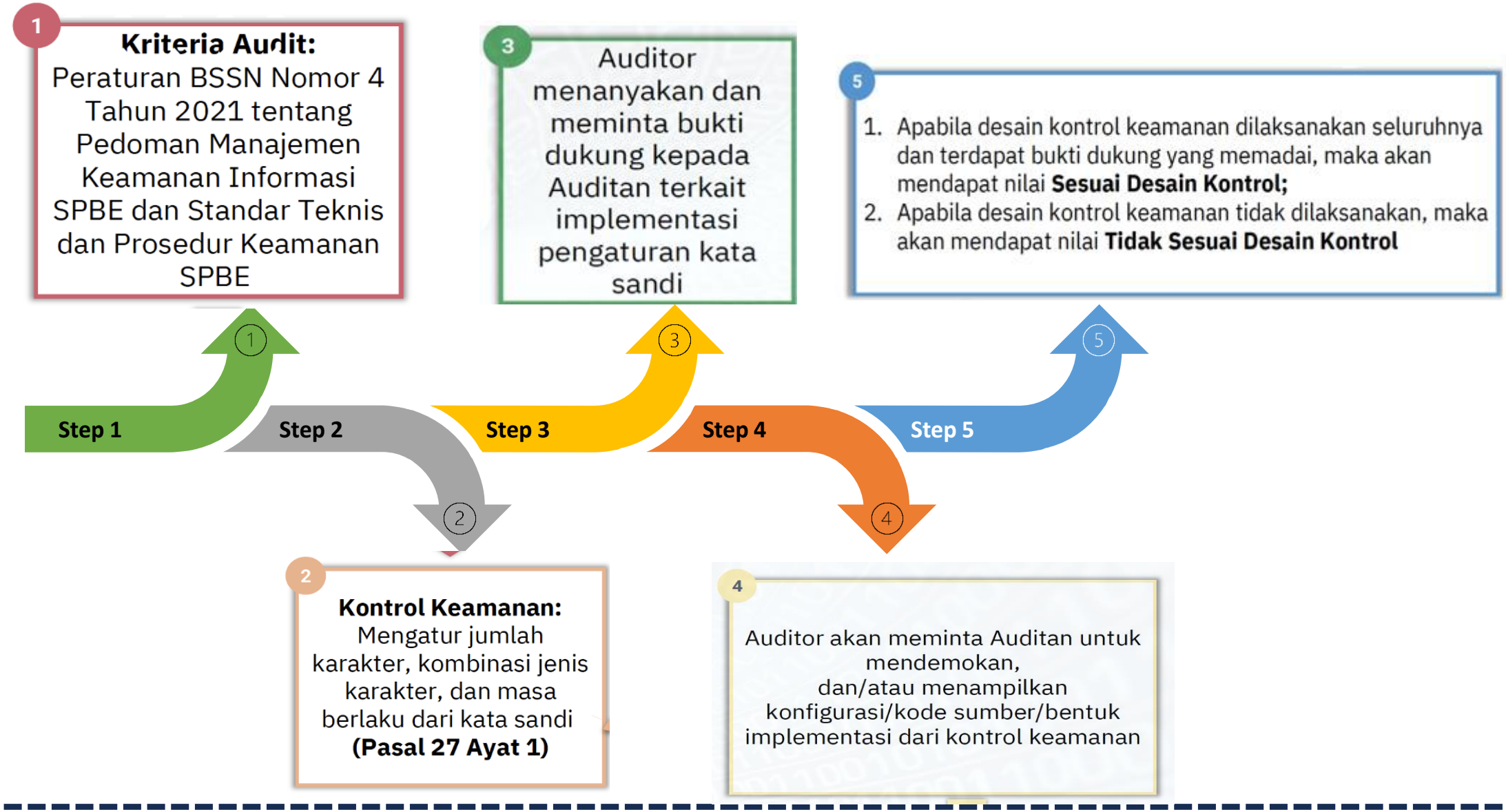
Kontrol Keamanan:
Mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi **(Pasal 27 Ayat 1)**

4

Auditan memberikan peraturan atau kebijakan yang terkait tentang mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi kepada Auditor.

BADAN SIBER DAN SANDI NEGARA

CONTOH: EVALUASI IMPLEMENTASI KONTROL AREA STANDAR TEKNIS



CONTOH: EVALUASI EFEKTIVITAS KONTROL AREA STANDAR TEKNIS

FUNGSI AUTENTIKASI

Kontrol (Peraturan BSSN 4/2021)

- **Pasal 27 ayat (1) huruf c**
  Mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi
- **Pasal 27 ayat (1) huruf d**
  Mengatur jumlah maksimum kesalahan dalam memasukkan kata sandi

Pengujian

- Melakukan *bruteforce/dictionary* attack pada login form aplikasi
- *Dictionary/wordlist* yang digunakan adalah daftar password lemah

Hipotesis

- Jika serangan berhasil maka aplikasi masih menerima *password* lemah. Karakter *password* lemah umumnya pendek, tidak menggunakan kombinasi dan mudah ditebak.
- Jika selama serangan tidak di *banned*, maka aplikasi belum menerapkan maksimal kesalahan dalam pemasukkan kata sandi

BADAN SIBER DAN SANDI NEGARA

TENTANG INTERNAL AUDIT

Definisi Audit Internal menurut Standar Audit APIP *adalah seluruh proses kegiatan audit, reviu, pemantauan, evaluasi dan kegiatan pengawasan lainnya berupa* ***asistensi, sosialisasi dan konsultansi*** *terhadap penyelenggaraan fungsi dan organisasi dalam memberikan keyakinan yang memadai bahwa kegiatan telah dilaksanakan sesuai tolok ukur yang telah ditetapkan secara* ***efektif dan efisien*** *untuk kepentingan pimpinan dalam mewujudkan* ***kepemerintahan yang baik***

Persamaan Audit Internal & Eksternal

1. Dilakukan oleh personil yang harus independen terhadap proses, area atau unit kerja yang dilakukan audit
2. Bertujuan untuk memberikan rekomendasi dan jaminan atas desain dan efektifitas operasional
3. Berpedoman pada standar audit
4. Melakukan pembandingan antara fakta-fakta yang dijumpai di pihak auditi dengan kriterianya
5. Akses terhadap Data dan sumber daya yang diperlukan pada saat proses audit tidak boleh dibatasi

Perbedaan Audit Internal & Eksternal

Audit Internal	Audit Eksternal
• Auditor dari Internal Organisasi	• Auditor dari Luar Organisasi
• Audit dilakukan pada sepanjang tahun	• Audit dilakukan terbatas pada waktu tertentu
• Memberikan umpan balik dan berorientasi pada perbaikan operasi	• Untuk menyatakan pendapat independen, memberikan penilaian akhir dan berorientasi pada kepatuhan terhadap standar

BADAN SIBER DAN SANDI NEGARA

HASIL DAN RENCANA AKSI PERSIAPAN AUDIT INTERNAL

Hasil Audit Internal

- **Tujuan** — Menetapkan tingkat kesesuaian antara aspek keamanan dengan kriteria dan/atau standar yang telah ditetapkan
- **Temuan** — Rincian aspek yang belum sesuai berdasarkan seluruh unsur SPBE, mulai Tata Kelola, Manajemen, Fungsional aplikasi, kinerja aplikasi dan aspek TIK lainnya. (sesuai Perpres SPBE)
- **Rekomendasi** — Apa yang harus diperbaiki sesuai standar, peraturan perundangan untuk mencapai tujuan SPBE
- **Tindak Lanjut** — Jangka waktu penyelesaian

Rencana Aksi Persiapan Audit Internal

1. Menetapkan tim audit internal : AUDITOR dan AUDITEE sesuai domain audit (SK Tim Audit)
2. Melihat kembali peraturan SPIP (APIP/Auditor memimpin pelaksanaan audit internal SPBE)
3. Mempelajari Instrumen Audit
4. Melakukan pembekalan bagi auditor dan auditee
5. Kegiatan Audit Internal tidak dilakukan menunggu penerapan keamanan IT telah dilaksanakan sempurna

BADAN SIBER DAN SANDI NEGARA

LANGKAH PEMENUHAN INDIKATOR 31 (AUDIT KEAMANAN SPBE)

01 Menyusun kebijakan SMKI merujuk Perban BSSN No 4/2021 dan SNI/ISO 27001

02 Menyusun Peta Rencana Keamanan SPBE dengan memasukkan Audit Keamanan SPBE sebagai kegiatan rutin yang berkesinambungan.

03 Menyusun pedoman audit keamanan SPBE (untuk keperluan audit internal).

04 APIP melakukan audit internal dan menghasilkan LHA Audit Internal

05 Jika Instansi sudah melakukan audit internal keamanan SPBE dan akan melakukan audit eksternal keamanan SPBE, sementara ekosistem LATIK Terakreditasi belum tersedia, maka dapat mengajukan permohonan audit keamanan SPBE kepada BSSN dengan catatan sbb:

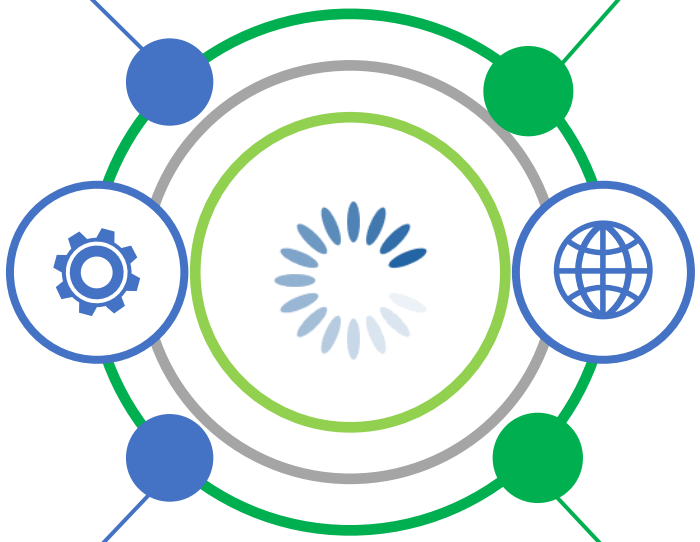
- ✓ pastikan sudah ada LHA audit internal yang dilakukan oleh Inspektorat (APIP).
- ✓ pastikan objek audit eksternal yang diajukan sama dengan objek audit internal yang telah dilakukan oleh Inspektorat (APIP).

- ❑ LATIK Terakreditasi melakukan audit eksternal dan menghasilkan LHA Audit Eksternal. Namun karena saat ini ekosistem LATIK Terakreditasi belum ada, maka berdasarkan Permenkominfo No 16 Th 2022 Pasal 16 Ayat (8), maka audit eksternal dapat dilakukan oleh LATIK Pemerintah (BSSN)
- ❑ Audit internal keamanan SPBE dapat menggunakan pedoman audit internal yang berlaku di masing-masing instansi. Perbedaan hanya pada objek dan kriteria audit yang digunakan.
- ❑ Hasil Audit internal cukup menyampaikan temuan dan rekomendasi saja (tidak perlu sampai kesimpulan memadai / tidak memadai / perlu peningkatan).

KESIMPULAN

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten
Harmonis Loyal Adaptif Kolaboratif

- Dasar hukum Audit TIK merujuk Perpres 95/2018 yang diturunkan menjadi Perkominfo Kupatik dan menjadi **delegasi penyusunan RPBSSN tentang STA Keamanan SPBE**
- 3 Indikator Keamanan SPBE saling terkait sehingga perlu dukungan dalam rangka **penerapan SPBE yang mengutamakan prinsip** *secure by design*



- Pelaksanaan Audit Keamanan terdiri dari **evaluasi desain, evaluasi implementasi dan evaluasi efektifitas**
- Dalam hal pelaksanaan Audit **Keamanan untuk kebutuhan internal** tidak menghasilkan kesimpulan hanya **rekomendasi perbaikan**

"Ingatlah bahwa kechilafan
satu orang sahaja tjukup sudah
menjebabkan keruntuhan negara."

dr. Roebiono Kertopati
Bapak Persandian Indonesia

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Terima kasih