



# Audit Keamanan SPBE

Danang Jaya

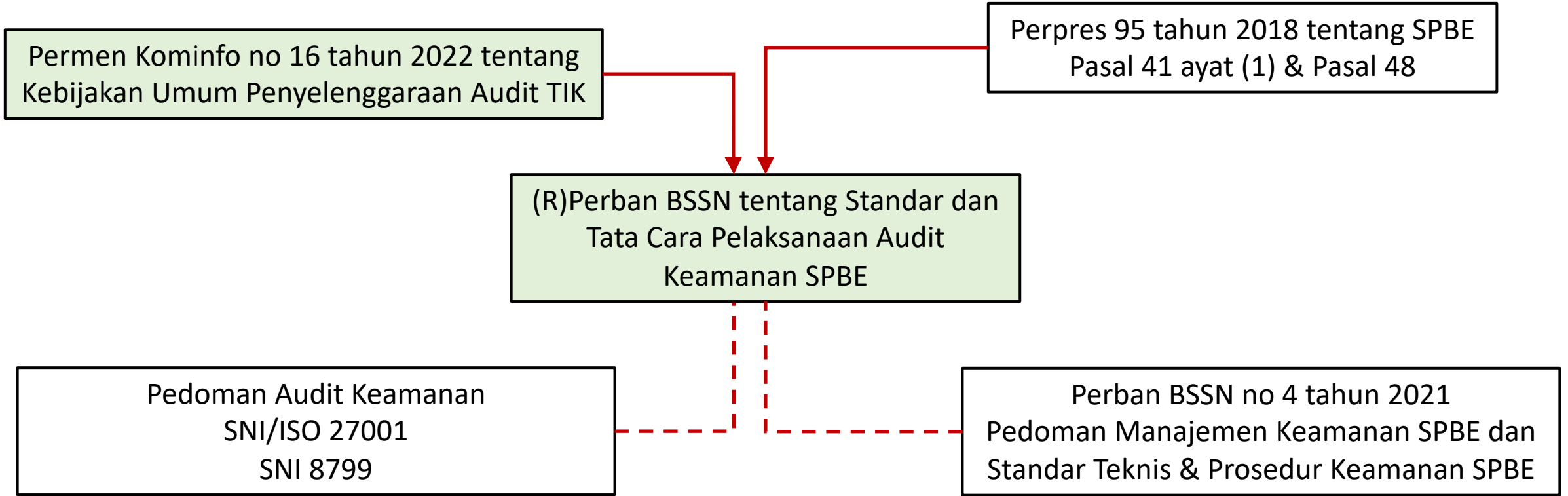
Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemerintah Pusat

Disampaikan pada Bimtek Permen KUPATIK, 9 Juli 2023



# Tata Kelola Audit Keamanan SPBE

Audit Teknologi Informasi dan Komunikasi yang selanjutnya disebut Audit TIK adalah proses yang sistematis untuk **memperoleh dan mengevaluasi bukti** secara objektif terhadap aset TIK dengan tujuan untuk **menetapkan tingkat kesesuaian** antara TIK dengan kriteria dan/atau standar yang telah ditetapkan





# Latar Belakang

PSE wajib menjamin Keamanan Infomasi



## Permenpan Nomor 59 Tahun 2020

Indikator 9	tingkat kematangan kebijakan internal audit teknologi informasi dan komunikasi
-------------	--

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

## Perpres Nomor 95 Tahun 2018

Pasal 58

- (1) Audit keamanan SPBE terdiri atas:
  - a. audit keamanan Infrastruktur SPBE Nasional;
  - b. audit keamanan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah;
  - c. audit keamanan Aplikasi Umum; dan
  - d. audit keamanan Aplikasi Khusus.
- (2) Audit keamanan SPBE sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan standar dan tata cara pelaksanaan audit Keamanan SPBE.

## Permen Kominfo no 16 tahun 2022 tentang Kebijakan Umum Penyelenggaraan Audit TIK

Pasal 5

Audit TIK meliputi pemeriksaan hal pokok teknis pada:

- a. penerapan tata kelola dan manajemen TIK;
- b. fungsionalitas TIK;
- c. kinerja TIK yang dihasilkan; dan
- d. aspek TIK lainnya.

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.

## RPB BSSN tentang Standar & Tata Cara Pelaksanaan Audit Keamanan SPBE

Pasal 3

Standar Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 2 huruf a terdiri atas:

- a. standar umum;
- b. standar pelaksanaan;
- c. standar pelaporan; dan

Pasal 4

- (1) Standar umum sebagaimana dimaksud dalam Pasal 3 huruf a memberikan prinsip dasar untuk mengatur Auditor pada LATIK Pemerintah serta LATIK Terakreditasi dan Terdaftar dalam melaksanakan tugas untuk menerapkan standar pelaksanaan, dan standar pelaporan secara efektif.
- (2) Standar umum sebagaimana dimaksud pada ayat (1) terdiri atas:
  - a. unsur Audit Keamanan SPBE;
  - b. etika Auditor;
  - c. prinsip Audit Keamanan SPBE.
- (2) Pelaksanaan audit keamanan SPBE oleh unit kerja yang memiliki fungsi pengawasan internal sebagaimana dimaksud pada ayat (1) tidak menghilangkan kewajiban Audit Keamanan SPBE yang dilakukan oleh LATIK Pemerintah dan LATIK Terakreditasi dan Terdaftar.

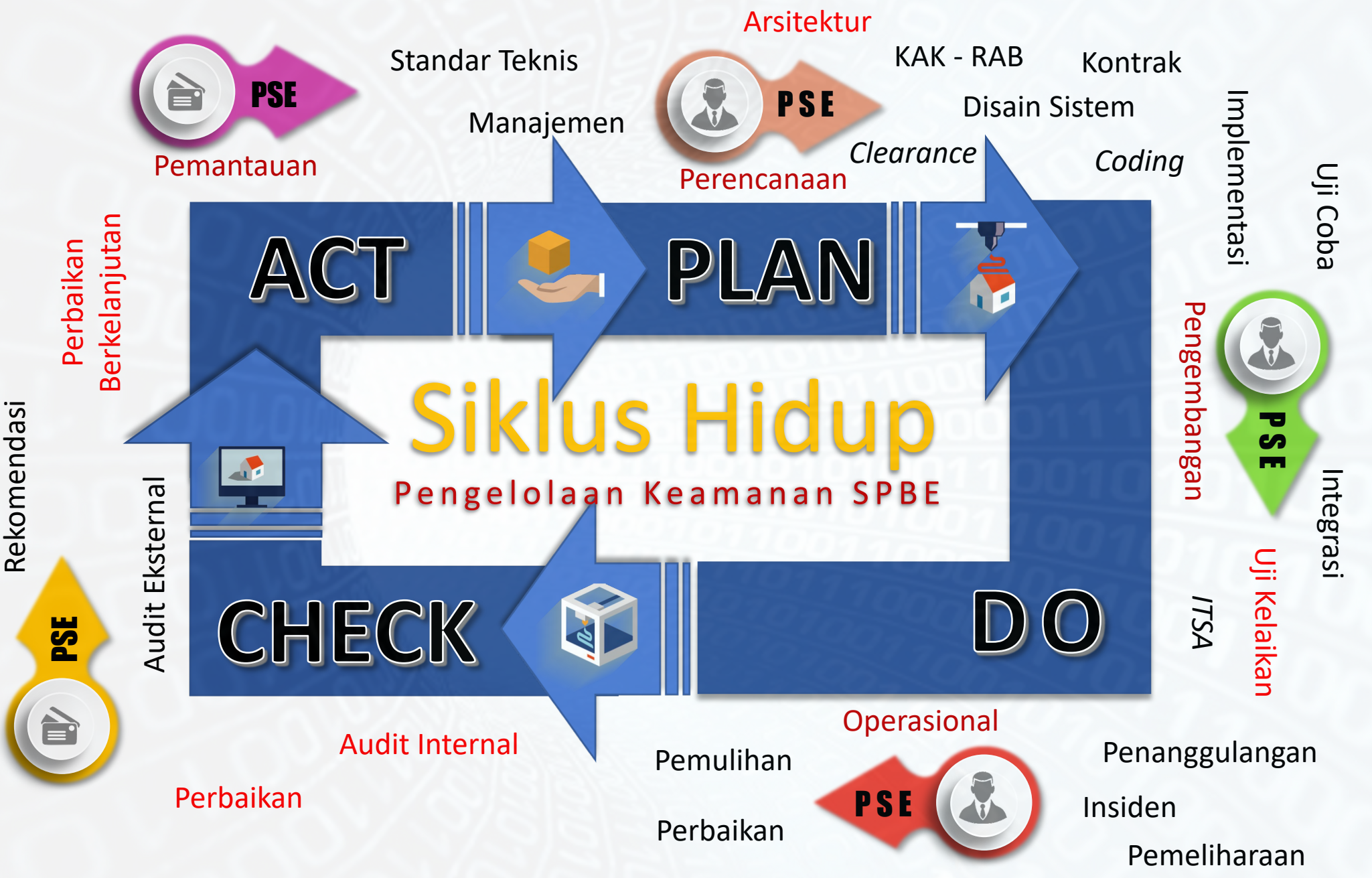


# Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

Apakah Instansi 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.









# Pengaturan (R)Perban BSSN tentang Standar & Tata Cara Pelaksanaan Audit Keamanan

Ver. 19 Juli 2021

RANCANGAN PERATURAN BADAN SIBER DAN SANDI NEGARA  
NOMOR TAHUN 2021  
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;

Mengingat : 1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);  
2. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);  
3. Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2020 Nomor 1464);  
4. Permenkominfo Audit TIK...

Ver. Maret 2023

RANCANGAN PERATURAN BADAN SIBER DAN SANDI NEGARA  
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

Mengingat : 1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);  
2. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);  
3. Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);  
4. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja

**Cat. Ver:**  
Biru = Perubahan hasil Le...  
Orange = Perubahan hasil... Desember 2022  
Hijau = Pembahasan hasil Januari 2023  
Ungu = Pembahasan hasil Februari dan Maret 2023  
Kuning = Catatan atau perlu dibahas lebih lanjut

Sedang dilakukan penyesuaian, pembaharuan sampai 27 Maret 2023 akan ditandai

## SUBSTANSI MATERI PENGATURAN

1. STANDAR AUDIT KEAMANAN SPBE
  1. Ruang Lingkup
  2. Pelaksana
  3. Hal Pokok Teknis
2. TATA CARA AUDIT KEAMANAN SPBE
  1. Tahapan Pelaksanaan
  2. Sumber Daya Audit Keamanan Spbe







# Ruang Lingkup & Pelaksana



➔ 1 kali dalam 1 tahun

IPPD MELALUI LEMBAGA PELAKSANA AUDIT TERAKREDITASI

➔ minimal 1 kali dalam 2 tahun

<h3>Pelaksana Audit Eksternal</h3> <hr/> <p><b>BSSN</b> sebagai Lembaga Audit TIK Pemerintah</p> <ul style="list-style-type: none"><li>- Aplikasi Umum dan Infrastruktur SPBE Nasional</li><li>- Aplikasi Khusus Infrastruktur IP, dan Infrastruktur PD yang dikecualikan*</li></ul>	<p><b>LAKI</b> bidang SPBE yang terakreditasi</p> <p>Aplikasi Khusus, Infrastruktur IP, dan Infrastruktur PD</p> <p><small>*Pengecualian tersebut ditetapkan dalam Keputusan Kepala Badan</small></p>
<p>Pelaksana Audit Internal (IP dan PD)</p>	





# Area Audit Keamanan SPBE

## Fungsionalitas Keamanan

- Kelengkapan Fungsi Keamanan
- Kebenaran Fungsi Keamanan
- Kelayakan Fungsi Keamanan



## Tata Kelola Keamanan

- Pengevaluasian
- Pengarahan
- Pemantauan



## Dapat memperhatikan

- SNI
- Standar Internasional
- Peraturan lain terkait kaminfo & perlindungan privasi



## Manajemen Keamanan



### Sistem Manajemen Keamanan

- Perencanaan
- Pengembangan
- Pengoperasian
- Pemantauan

### Pengendalian Keamanan

- Organisasi Keamanan
- Keamanan Personil
- Keamanan Fisik
- Keamanan Teknologi





# MATRIKS KESIMPULAN AUDIT KEAMANAN SPBE

Hasil Evaluasi Desain Pengendalian	Hasil Evaluasi Implementasi Pengendalian	Hasil Pengujian Terinci Efektivitas Pengendalian	Kesimpulan Audit Keamanan SPBE
<b>Memadai</b>	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
<b>Perlu Peningkatan</b>	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
<b>Tidak Memadai</b>	-	Efektif	Tidak Memadai
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai





# Pelaksanaan

auditor melakukan langkah-langkah untuk mengidentifikasi informasi terdokumentasi untuk memperoleh pemahaman yang memadai tentang **pengendalian keamanan**



auditor melakukan langkah-langkah untuk memperoleh keyakinan yang memadai bahwa desain pengendalian Keamanan SPBE telah sesuai dengan kriteria yang digunakan





# Pelaksanaan

auditor melakukan langkah-langkah untuk memperoleh keyakinan yang memadai bahwa pengendalian Keamanan SPBE telah dapat mencapai tujuannya dengan efektif



auditor melakukan langkah-langkah untuk memperoleh keyakinan yang memadai bahwa implementasi pengendalian Keamanan SPBE telah sesuai dengan desain pengendalian yang ada



# Pemetaan Waktu Audit

Kompleksitas Domain	Kompleksitas Teknologi	Sebaran Lokasi	Jumlah Hari (paling sedikit)
Sederhana	Sederhana	Terpusat	2
		Tersebar	3
	Sedang	Terpusat	3
		Tersebar	4
	Kompleks	Terpusat	4
		Tersebar	5
Sedang	Sederhana	Terpusat	5
		Tersebar	6
	Sedang	Terpusat	6
		Tersebar	7
	Kompleks	Terpusat	7
		Tersebar	8
Kompleks	Sederhana	Terpusat	8
		Tersebar	9
	Sedang	Terpusat	9
		Tersebar	10
	Kompleks	Terpusat	10
		Tersebar	10





# Pemetaan Profil Audit

Informasi Umum Domain Audit Keamanan SPBE			
A. Jenis	Sederhana	Sedang	Kompleks
Aplikasi SPBE	Aplikasi Khusus Instansi Pusat	Aplikasi Khusus Pemerintah Daerah	Aplikasi Umum SPBE Nasional
Pusat Data Nasional	Instansi Pusat	Pemerintah Daerah	Nasional
Jaringan Intra	Instansi Pusat	Pemerintah Daerah	Nasional
Sistem Penghubung Layanan	Instansi Pusat	Pemerintah Daerah	Nasional
B. Umum			
Jumlah Personil TI	< 5 orang	6-10 orang	> 10 orang
Jumlah Pengguna	< 100 pengguna	100-1000 pengguna	> 1000 pengguna
Jenis Dampak Kegagalan	Operasional saja	Operasional dan Finansial	Operasional, Finansial, dan Legal
C. Aplikasi SPBE			
Sebaran peladen	Terpusat	Terdistribusi Dalam Negeri	Terdistribusi Dalam & Luar Negeri
Platform Teknologi	1 jenis	2-3 jenis	> 3 jenis
Waktu Pengembangan	< 3 bulan	3-12 bulan	> 12 bulan
Usia Sistem	< 1 tahun	1-3 tahun	> 3 tahun
Transaksi per hari	< 5000	5000 s.d. 50.000	> 50.000
Pola Pemrosesan	<i>Batch</i>	<i>Realtime</i>	<i>Hybrid</i>
Cakupan Proses Bisnis	< 30 %	30-60%	> 60%
D. Pusat Data Nasional			
Pengelolaan	Alih Daya, Sewa	Mandiri	Campuran
Strata SNI	Strata 1-2	Strata 3	Strata 4
Sertifikasi	Belum Ada	SNI 27001	SNI 27001 dan Standar Lain
E. Jaringan Intra			
Pengelolaan	Alih Daya, Sewa	Mandiri	Campuran
Cakupan Jaringan	<i>Local Area Network , Campus Area Network</i>	<i>Metropolitan Area Network, Virtual Private Network</i>	<i>Wide Area Network , Nasional</i>
Media Jaringan	Kabel	Nirkabel	Kabel & Nirkabel
F. Sistem Penghubung Layanan			
Cakupan Sistem	Intra Instansi Pusat atau Intra Pemerintah Daerah	Antar Instansi Pusat atau Antar Pemerintah Daerah	Nasional
Sifat Sistem	Tertutup	Semi Terbuka	Terbuka
Konten Sistem	Data	Aplikasi	Layanan
Sifat Informasi	Terbuka	Terbatas	Tertutup



# Tata Cara Pelaksanaan Audit Keamanan SPBE

## PERMINTAAN

- Hanya untuk audit yang dilaksanakan LAKI bidang SPBE yang terakreditasi
- Dilakukan dengan mengirimkan Surat Permintaan Audit Keamanan SPBE



## PENUGASAN

- Dilakukan menerbitkan Surat Tugas Audit Keamanan SPBE



## PERENCANAAN

- menyusun Perencanaan Audit Keamanan SPBE



## PELAKSANAAN

- prosedur pemahaman pengendalian
- prosedur evaluasi desain pengendalian
- prosedur pengujian implementasi pengendalian
- prosedur pengujian terinci efektivitas pengendalian



## SUPERVISI

- supervisi aspek mutu
- supervisi aspek teknis



## PELAPORAN

- dilakukan dengan menyusun Laporan Audit Keamanan SPBE



## TINDAK LANJUT

- Dilakukan oleh Auditor Keamanan SPBE berikutnya atau Instansi Pusat dan Pemerintah Daerah







Jadikan **Keamanan** sebagai syarat dasar untuk mendapatkan  
**Kenyamanan**

**Karena tanpa keamanan tidak akan ada kenyamanan**