Peningkatan Kualitas Keamanan SPBE

Danang Jaya

Direktur Keamanan Siber dan Sandi Pemerintah Daerah

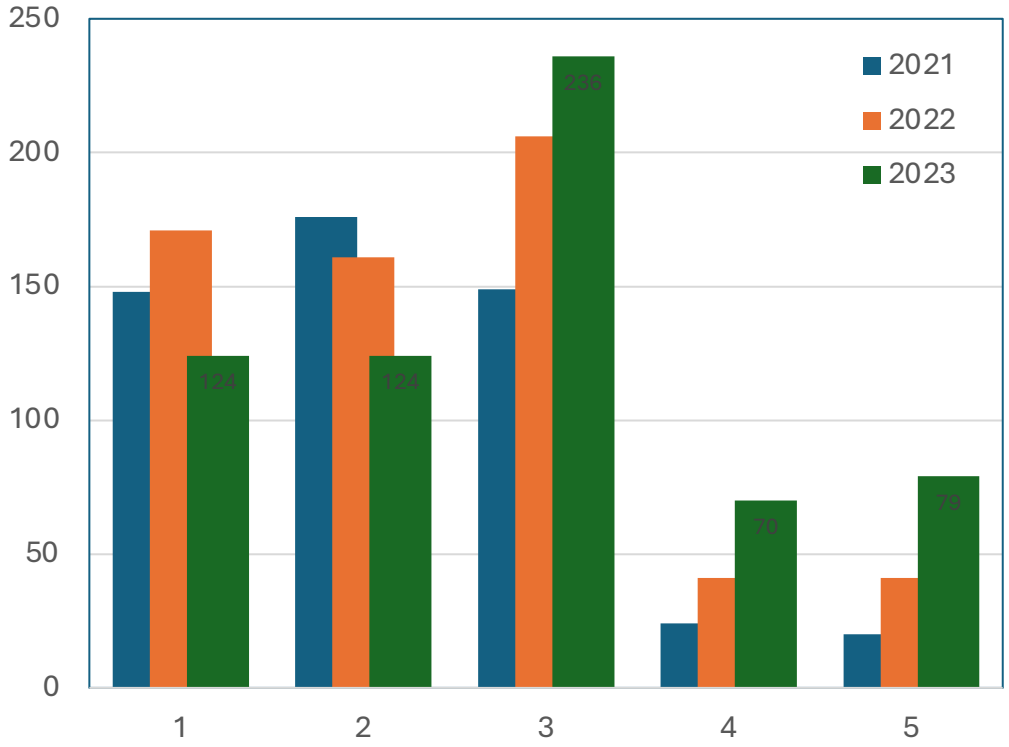
Disampaikan pada *Evaluasi SPBE Nasional*, 17 Juli 2024

Indikator Keamanan SPBE

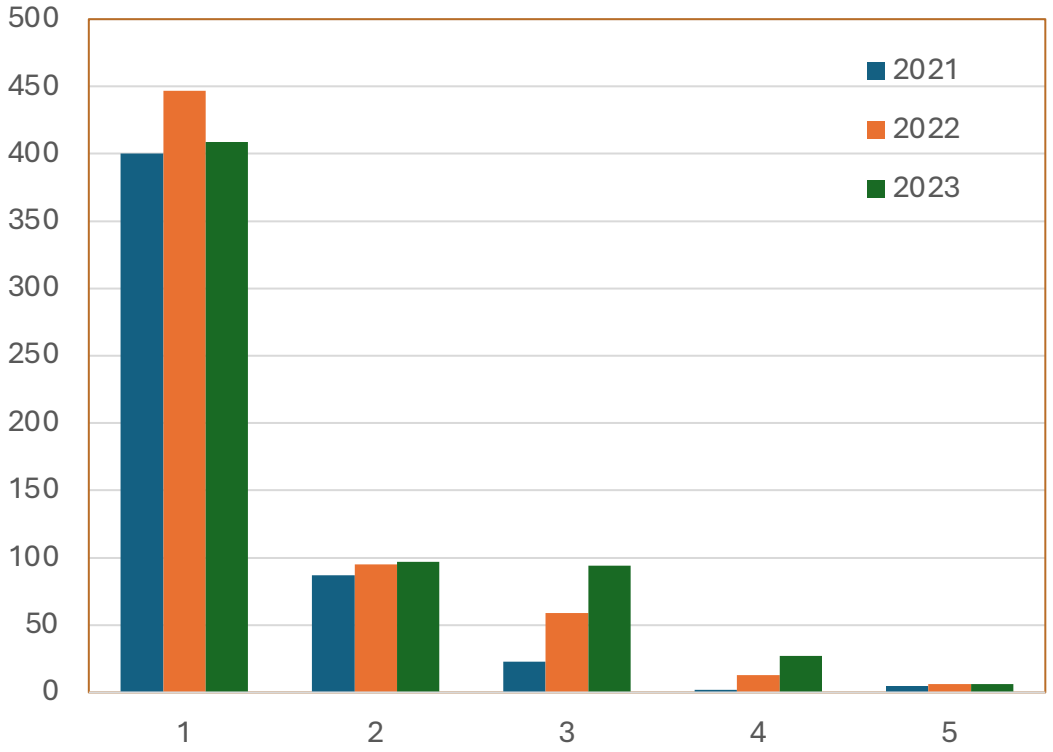
PESERTA

	IP	PD	TOTAL
2021	92	425	517
2022	96	524	620
2023	95	538	633

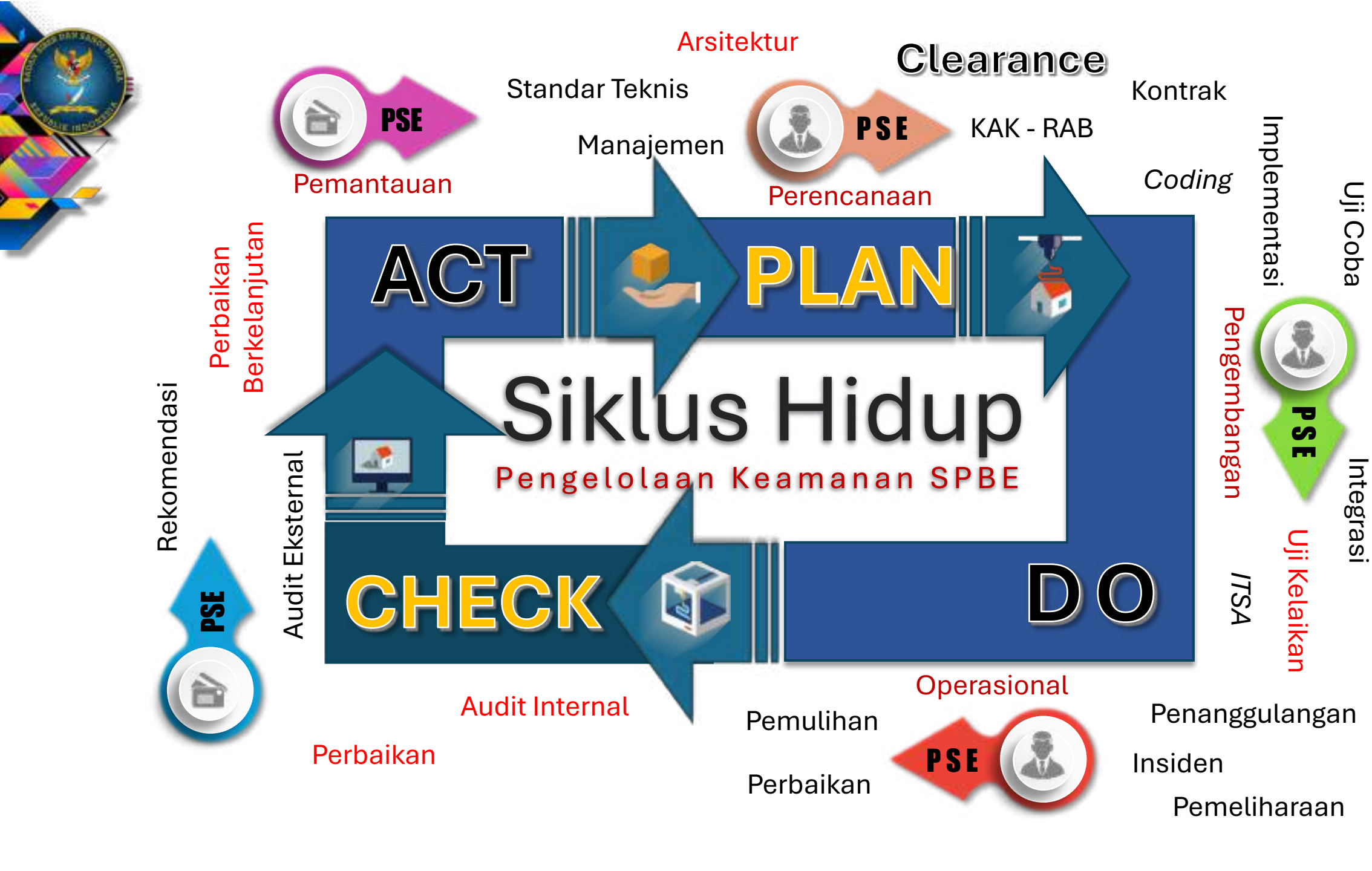
8 Kebijakan Internal Manajemen Keamanan Informasi



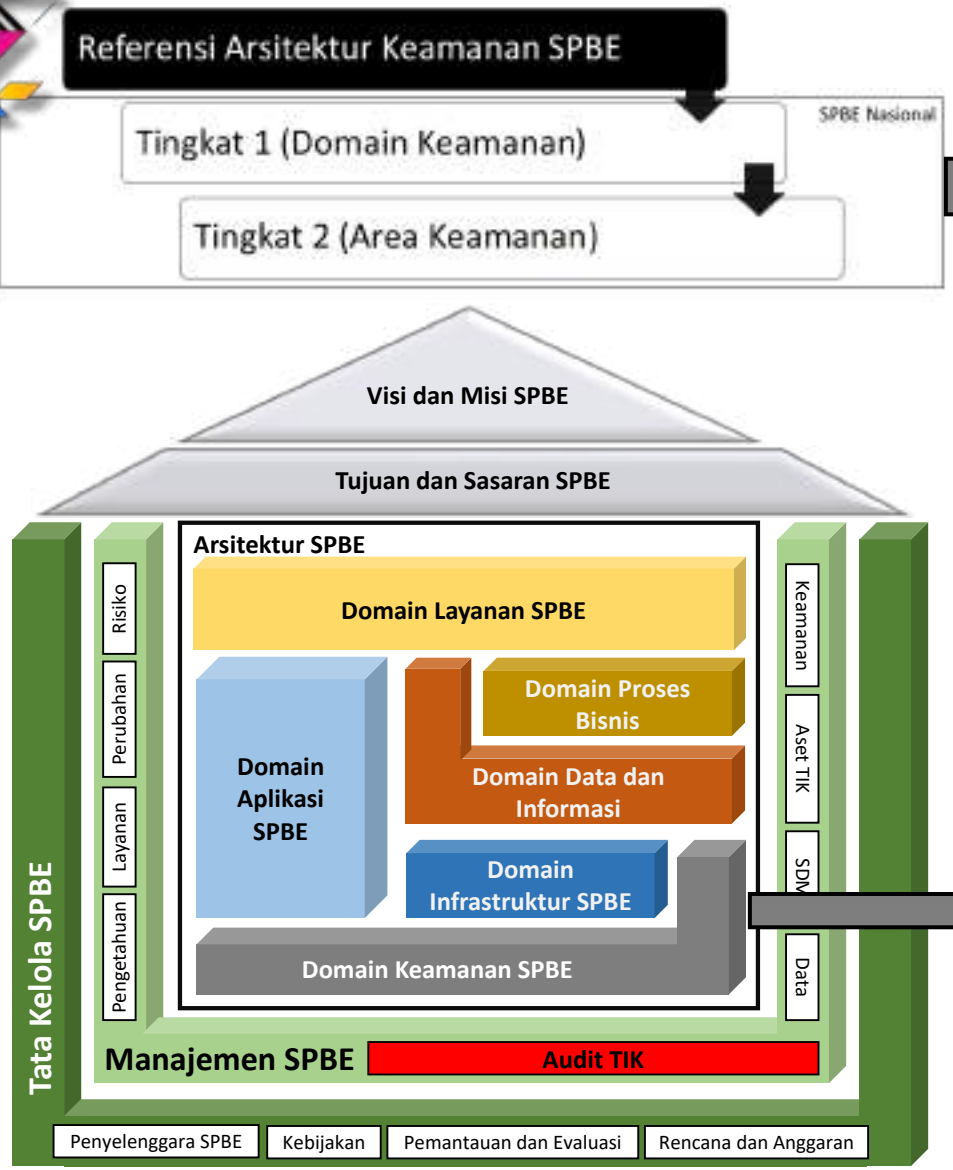
22 Penerapan Manajemen Keamanan Informasi




KEBIJAKAN
SISTEM MANAJEMEN KEAMANAN SPBE
8
AUDIT
KEAMANAN
31
ASET TIK
APLIKASI, INFRATRUKTUR & DATA
24
REVIEW KEAMANAN SPBE
PENERAPAN
MENGEDEPANKAN KEAMANAN DALAM KEGIATAN
22
RESIKO
MANAJEMEN RESIKO KEAMANAN SPBE
21
ARSITEKTUR
SECURITY BY DESIGN
1


Arsitektur
Clearance
Standar Teknis
Kontrak
Manajemen
KAK - RAB
Coding
Implementasi
Uji Coba
PSE
PSE
PSE
Pemantauan
Perencanaan
Perbaikan
Berkelanjutan
ACT
PLAN
Siklus Hidup
Pengelolaan Keamanan SPBE
Pengembangan
Integrasi
Rekomendasi
Audit Eksternal
CHECK
DO
ITSA
Uji Kelaikan
PSE
Operasional
Audit Internal
Pemulihan
Penanggulangan
PSE
Perbaikan
Insiden
Perbaikan
Pemeliharaan

Struktur Referensi Arsitektur Keamanan SPBE



•Referensi Arsitektur Keamanan SPBE

01 Standar Keamanan

- 01.01 Standar Teknis dan Prosedur Keamanan SPBE
- 01.02 Standar Keamanan Internasional
- 01.03 Regulasi lainnya

02 Penerapan Keamanan

- 02.01 Edukasi kesadaran Keamanan SPBE
- 02.02 Identifikasi kerentanan Keamanan SPBE
- 02.03 Peningkatan Keamanan SPBE
- 02.04 Penanganan insiden Keamanan SPBE
- 02.05 Audit Keamanan SPBE

03 Kelaikan Keamanan

- 03.01 Kelaikan Keamanan Aplikasi Umum
- 03.02 Kelaikan Keamanan Infrastruktur SPBE Nasional

Peraturan BSSN no 4 tahun 2021

Peraturan BSSN tentang Pedoman Manajemen Keamanan SPBE dan Standar Tehnis dan Prosedur Keamanan SPBE

- **Penetapan Ruang Lingkup**
- **Penanggung Jawab**
- **Perencanaan**
- **Dukungan Pengoperasian**
- **Evaluasi Keamanan**
- **Perbaikan berkelanjutan**

Standar Teknis dan Prosedur Keamanan

01
Data & Info
- Penerapan Eknripsi
- Pemanfaatan Seritifikat Elektronik
- Pemulihan & Pencadangan

02
Aplikasi
- Aplikasi berbasis Web
- Aplikasi Berbasis Desktop
- Aplikasi berbasis Mobile

03
PDN
Mengacu pada SNI / ISO 8799

04
JI
- Administrasi Jaringan
- Kontrol Akses dan Autentikasi
- Kontrol Keamanan

05
SPL
- Interoperabilitas
- Sistem Terintegrasi
- Perangkat Integrator
- API & Web Service

PERBAIKAN BERKELANJUTAN

Dari hasil evaluasi menjadi rekomendasi dalam perbaikan secara terus menerus

EVALUASI KINERJA

Untuk melihat efektivitas penerapan manajemen keamanan yang sudah ditetapkan

DUKUNGAN PENGOPERASIAN

Hal-hal yang perlu dipersiapkan dalam menjalankan keamanan seperti SDM, anggaran, kebijakan serta sumberdaya lainnya
Koordinator SPBE memberikan dukungan sumber daya berupa SDM dan anggaran

PENETAPAN RUANG LINGKUP

Hal-hal apa saja yang perlu diamankan terkait dengan isu internal dan eksternal.
Isu internal meliputi objek pengamanan yaitu data & informasi, aplikasi dan infrastruktur.

PENETAPAN PENANGGUNG JAWAB

Berdasarkan SOTK menetapkan penanggung jawab keamanan
Pimpinan Instansi menetapkan penanggung jawab

PERENCANAAN

Dalam menjalankan keamanan dapat menjawab program kerja keamanan
Disusun oleh pelaksana teknis keamanan berupa program kerja.

Templat Kebijakan SMKI SPBE

KEPALA BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA

NOMOR 499 TAHUN 2023

TENTANG

TEMPLAT KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : a. bahwa Sistem Manajemen Keamanan Informasi adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan;

b. bahwa template kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik ini merupakan alat bantu bagi Instansi Pemerintah dalam menyusun kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan b, perlu menetapkan Keputusan Kepala Badan Siber dan Sandi Negara tentang Template Kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik.

Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185);

3. Peraturan ....

Keputusan Kepala Badan Siber dan Sandi Negara

Nomor 499 tahun 2023

tentang

TEMPLAT KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

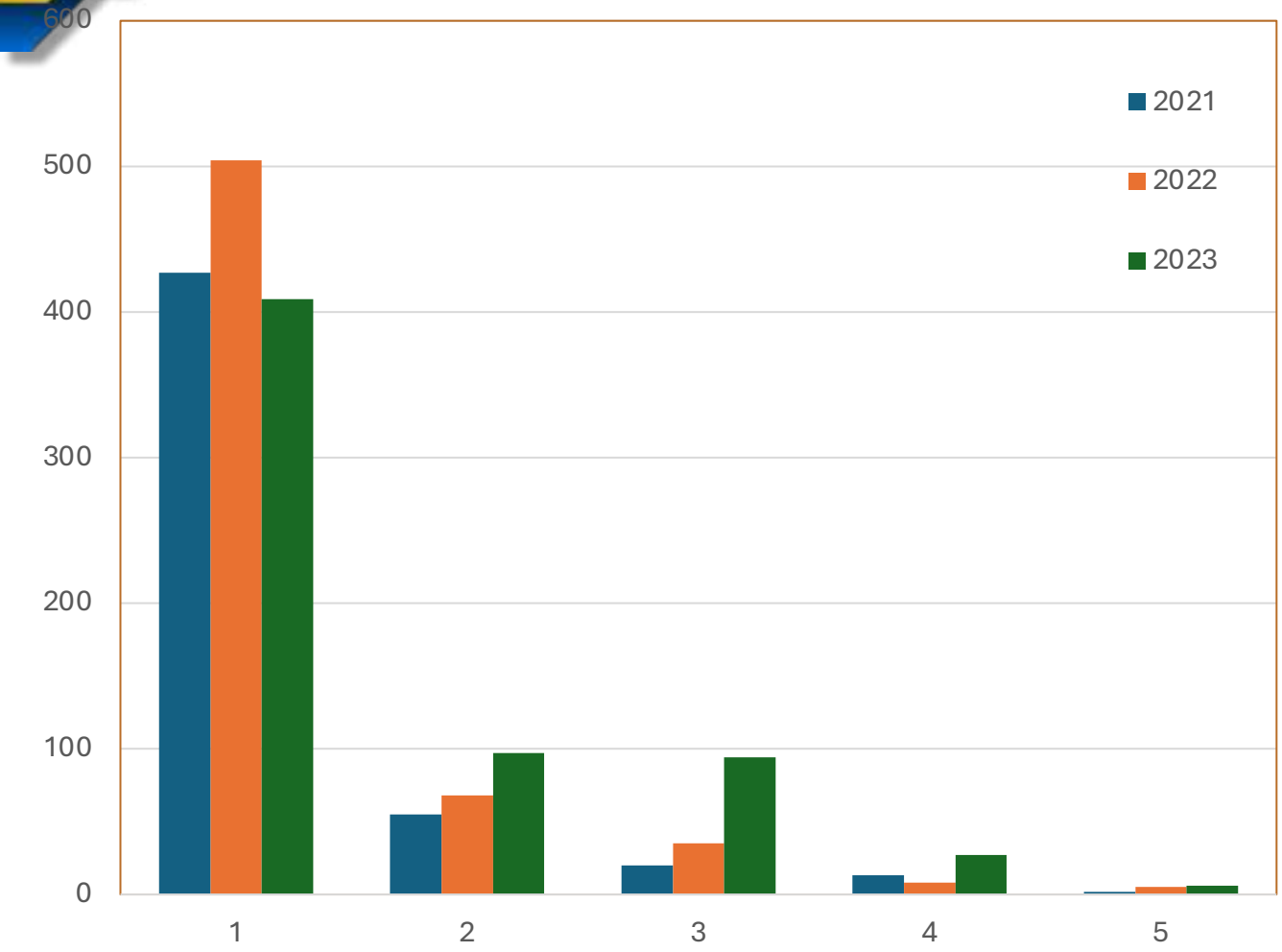
Surat plt Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia

Nomor 5451/BSSN/D3/PS.02.01/11/2022

tentang

Penyampaian Contoh Format Kebijakan Internal Manajemen Keamanan Informasi SPBE

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

Dasar Pelaksanaan Audit Keamanan SPBE

PERMENKOMINFO 16/2022

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.

Pasal 3

(1) Audit TIK pada lingkup nasional sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf a mencakup:
   a. audit Infrastruktur SPBE Nasional;
   b. audit Aplikasi Umum;
   c. audit keamanan Infrastruktur SPBE Nasional; dan
   d. audit keamanan Aplikasi Umum.
(2) Audit TIK pada lingkup Instansi Pusat dan Pemerintah Daerah sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf b dan huruf c mencakup:
   a. audit Infrastruktur SPBE;
   b. audit Aplikasi Khusus;
   c. audit keamanan Infrastruktur SPBE; dan
   d. audit keamanan Aplikasi Khusus.

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.

SEMESTA AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI SPBE

AUDIT INFRASTRUKTUR SPBE

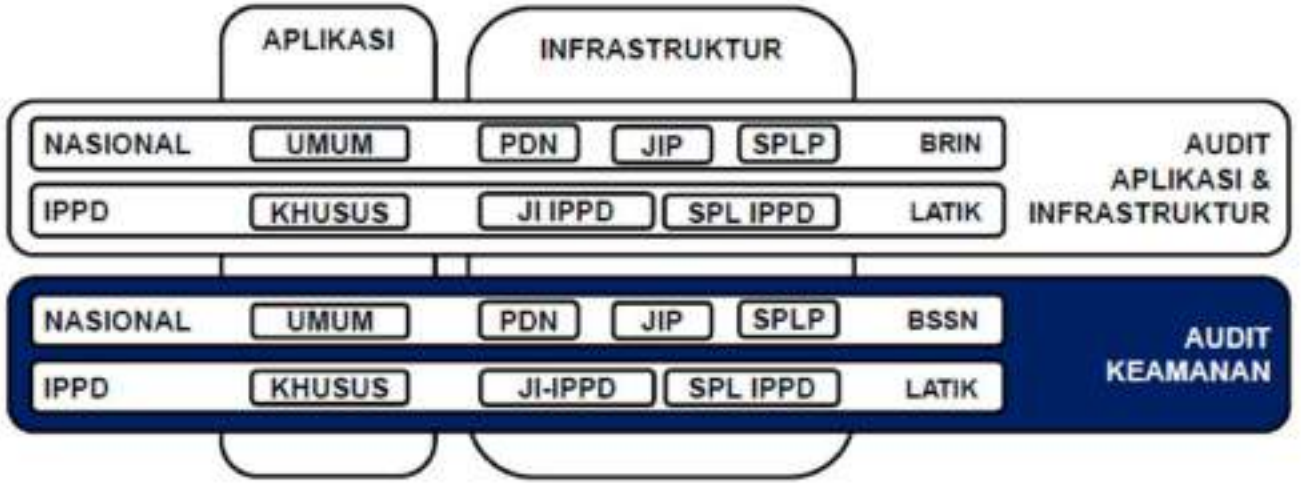
- Audit infrastruktur SPBE nasional
- Audit infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah.

AUDIT APLIKASI SPBE

Audit aplikasi umum dan audit aplikasi khusus.

AUDIT KEAMANAN SPBE

- Audit keamanan infrastruktur SPBE Nasional
- Audit keamanan infrastruktur SPBE IPPD,
- Audit keamanan aplikasi umum,
- Audit keamanan aplikasi khusus



1 (satu) kali dalam 1 (satu) Tahun

* Audit Keamanan Aplikasi Khusus dan Infra IPPD untuk Instansi Pusat Tertentu

INSTANSI PUSAT DAN PEMERINTAH DAERAH MELALUI LEMBAGA PELAKSANA AUDIT TERAKREDITASI

Paling sedikit 1 (satu) kali dalam 2 (dua) Tahun

Tujuan Audit Keamanan SPBE

1

TINGKAT KESESUAIAN

Pasal 1 Perpres Nomor 95/2018 ttg SPBE

Audit TIK BERTUJUAN untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan **kriteria dan/atau standar** yang telah ditetapkan.

2

KELAYAKAN DESAIN KONTROL DAN IMPLEMENTASI

Untuk memperoleh keyakinan yang memadai tentang kelayakan desain kontrol dan implementasi kontrol keamanan pada Aplikasi atau Infrastruktur.

Kriteria Audit Keamanan SPBE

PERATURAN PERUNDANG-UNDANGAN

KEBIJAKAN,KODE ETIK, STANDAR PRINSIP, SISTEM

PEDOMAN

JUKLAK/JUKNIS/SOP/STANDAR BERSIFAT OPERASIONAL/TEKNIS

DOKUMEN/PERANGKAT LAINNYA

Pasal 1 Permenkominfo No. 16 Tahun 2022

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.

Metode Audit Keamanan SPBE

KRITERIA AUDIT KEAMANAN

1. Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE
2. Keputusan Menteri PANRB Nomor XX Tahun XXX tentang Aplikasi Umum Bidang XXX
3. Referensi peraturan, standar, pedoman, juknis, dan/atau dokumentasi pendukung lainnya

LINGKUP AUDIT KEAMANAN

Objek Audit:

Aplikasi XX versi X

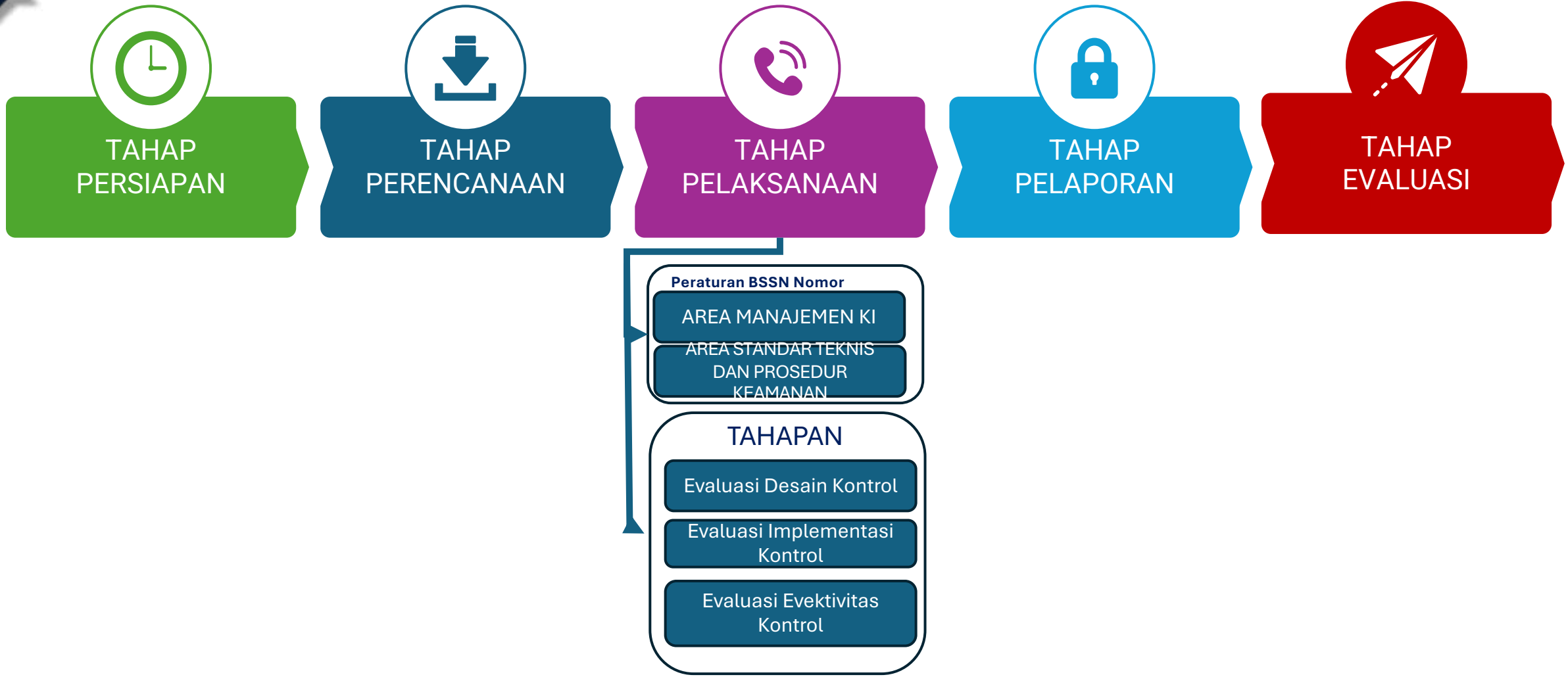
Periode Pemeriksaan:

Bulan 202X – Bulan 202X

TAHAPAN AUDIT KEAMANAN

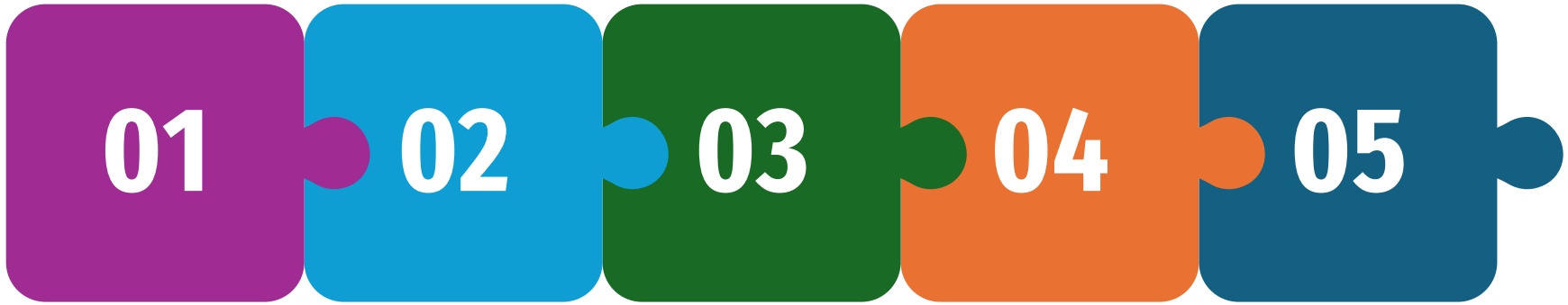
1. Tahap Pemahaman Kontrol Keamanan SPBE;
2. Tahap Evaluasi Desain Kontrol Keamanan SPBE
3. Tahap Evaluasi Implementasi Kontrol Keamanan SPBE; dan
4. Tahap Evaluasi Efektivitas Kontrol Keamanan SPBE

Proses Audit Keamanan SPBE



Prosedur Audit Keamanan SPBE

Standar Audit Keamanan SPBE



OBJEK AUDIT	PELAKSANA	KRITERIA	BUKTI	KESIMPULAN
objek Audit Keamanan SPBE	pelaksana Audit Keamanan SPBE	kriteria Audit Keamanan SPBE	bukti Audit Keamanan SPBE	kesimpulan Audit Kemanan SPBE

Pelaksana Audit Keamanan SPBE

PELAKSANA AUDIT EKSTERNAL

BSSN sebagai LATIK Pemerintah

> Aplikasi Umum dan Infrastruktur SPBE Nasional
> Aplikasi Khusus IP dan Infrastruktur yang dikecualikan*

LATIK Terakreditasi dan Terdaftar

> Aplikasi Khusus, Infrastruktur Instansi Pemerintah, dan Infrastruktur Pemerintah Daerah

Cakupan	Auditan	Waktu	Lembaga Audit	Auditor	Pedoman
Keamanan SPBE	Keamanan Infrastruktur SPBE Nasional	1 tahun sekali	BSSN	Auditor Keamanan SPBE BSSN	Standar & Tata Cara Audit dari BSSN
	Keamanan Infrastruktur SPBE IPPD	2 tahun sekali	LATIK	Auditor Keamanan SPBE LATIK	Standar & Tata Cara Audit dari BSSN
	Keamanan Aplikasi Umum	1 tahun sekali	BSSN	Auditor Keamanan SPBEi BSSN	Standar & Tata Cara Audit dari BSSN
	Keamanan Aplikasi Khusus	2 tahun sekali	LATIK	Auditor Keamanan SPBE LATIK	Standar & Tata Cara Audit dari BSSN

PELAKSANA AUDIT INTERNAL

Instansi Pusat dan Pemerintah Daerah

TERAKREDITASI di lembaga pemerintah nonstruktural yang bertugas dan bertanggung jawab di bidang akreditasi lembaga penilaian kesesuaian.
TERDAFTAR di BSSN.

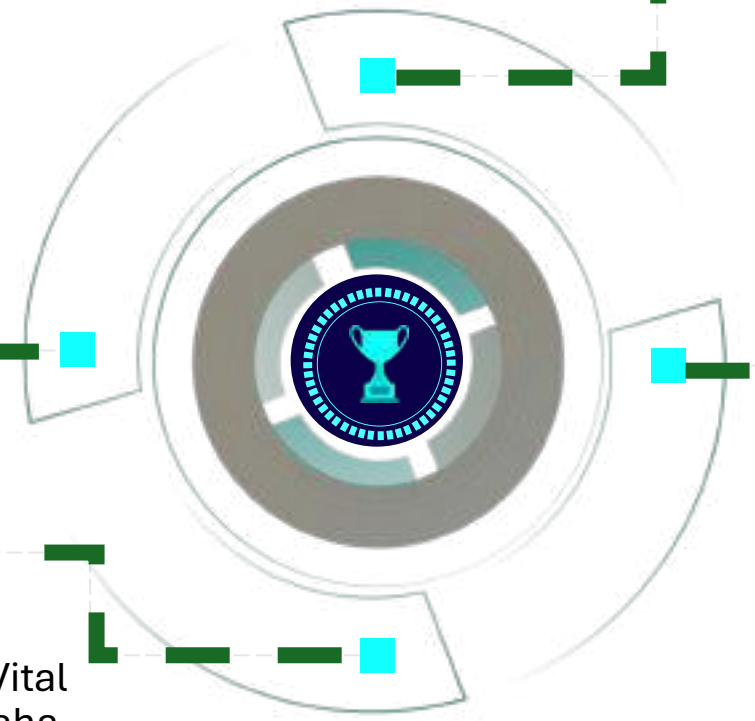
SISHANKAM(SIBER)RATA

INSTANSI PENYELENGGARA NEGARA

Mengembangkan kebijakan, strategi, dan regulasi terkait pembangunan Keamanan Siber di Indonesia dan memegang peran kepemimpinan dalam hal formulasi dan implementasi SKSN

AKADEMISI

Sebagai tulang punggung kemajuan sains, inovasi, dan teknologi bangsa Indonesia melalui kualitas pendidikan yang dapat memproduksi hasil-hasil riset, teknologi, dan sumber daya manusia yang berkualitas, transformatif, dan kompetitif dalam konteks menghadapi perkembangan ancaman dan tantangan keamanan siber di tingkat global



PELAKU USAHA

Mendorong keamanan Infrastruktur Informasi Vital (IIV), meningkatkan Keamanan Siber untuk Usaha Mikro Kecil dan Menengah (UMKM), menyediakan produk dan pelayanan yang aman di dunia siber, meningkatkan kemampuan para pekerja, dan menangkal upaya-upaya kejahatan siber dalam skala industri

KOMUNITAS

Mengaplikasikan pedoman dan informasi mengenai keamanan siber, melaporkan kejahatan siber, serta mendapatkan akses dan dukungan dari pemerintah sebagaimana dibutuhkan

STRATEGI KEAMANAN SIBER NASIONAL

Terapkan Security by Design

BUKAN Security By Insident atau Security By Accident