STANDAR MANAJEMEN KEAMANAN INFORMASI (SMKI) 27001:2022 DALAM PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI PEMERINTAH DAERAH

By Lukman Nul Hakim

Solo, 09 Februari 2023

AGENDA

SMKI Dalam Penyelenggaraan SPBE

- **Pengantar**
- **Pengertian SMKI dan SPBE**
- **Relevansi dan Keterhubungan antara SMKI dalam Penyelenggaraan SPBE**
- **BSSN dalam Keamanan Sistem Elektronik Tranformasi Digitital di Indonesia**
- **Implementasi SMKI dalam Penyelenggaraan SPBE Pemprov Jateng**
- **Penutup**

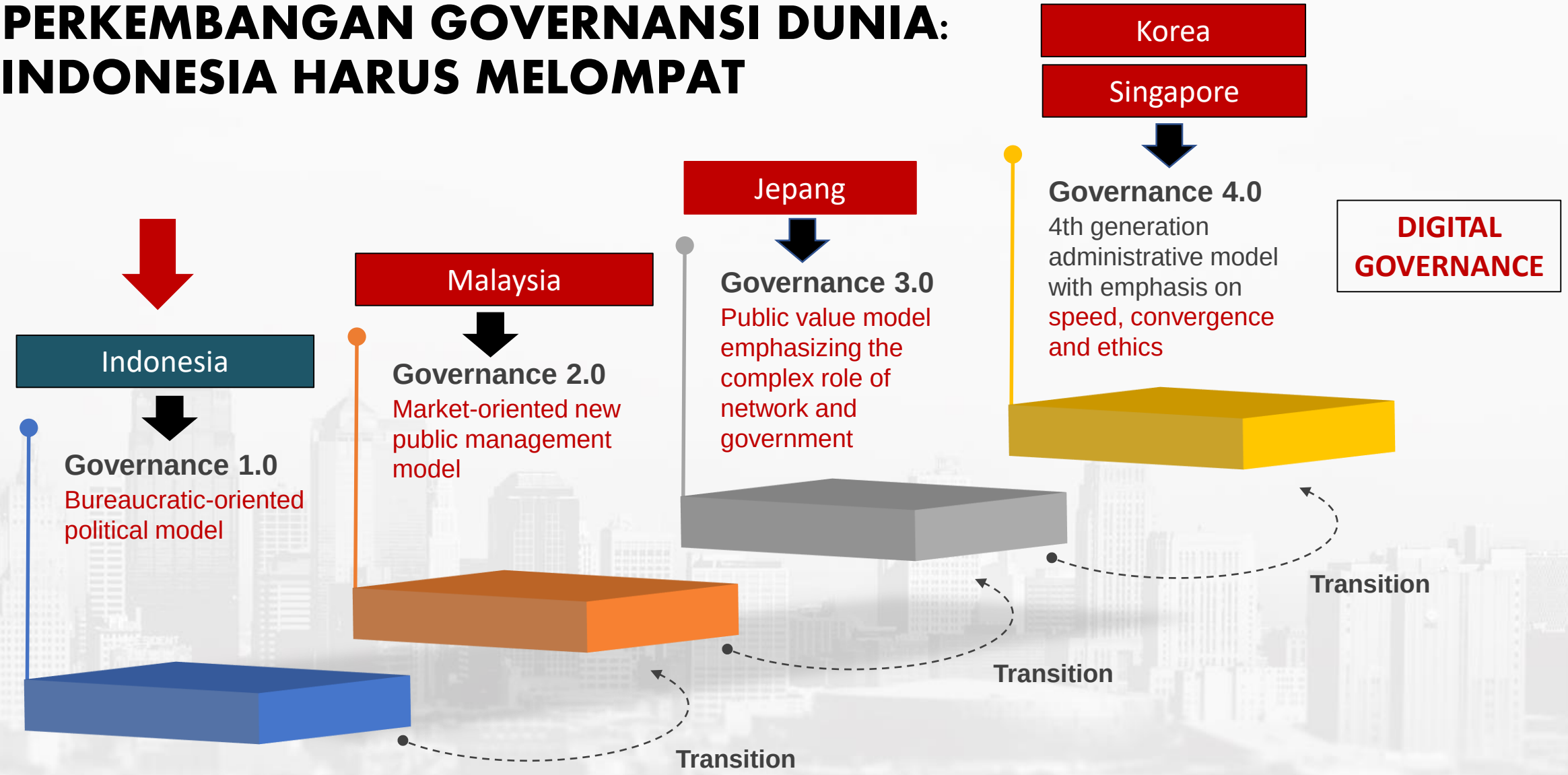
TIGA KEKUATAN PERUBAHAN

GLOBALISASI YANG MASIF DAN MENYELURUH
(Global Governance)

PERKEMBANGAN ICT DAN DISRUPSI
(Digital Governance)

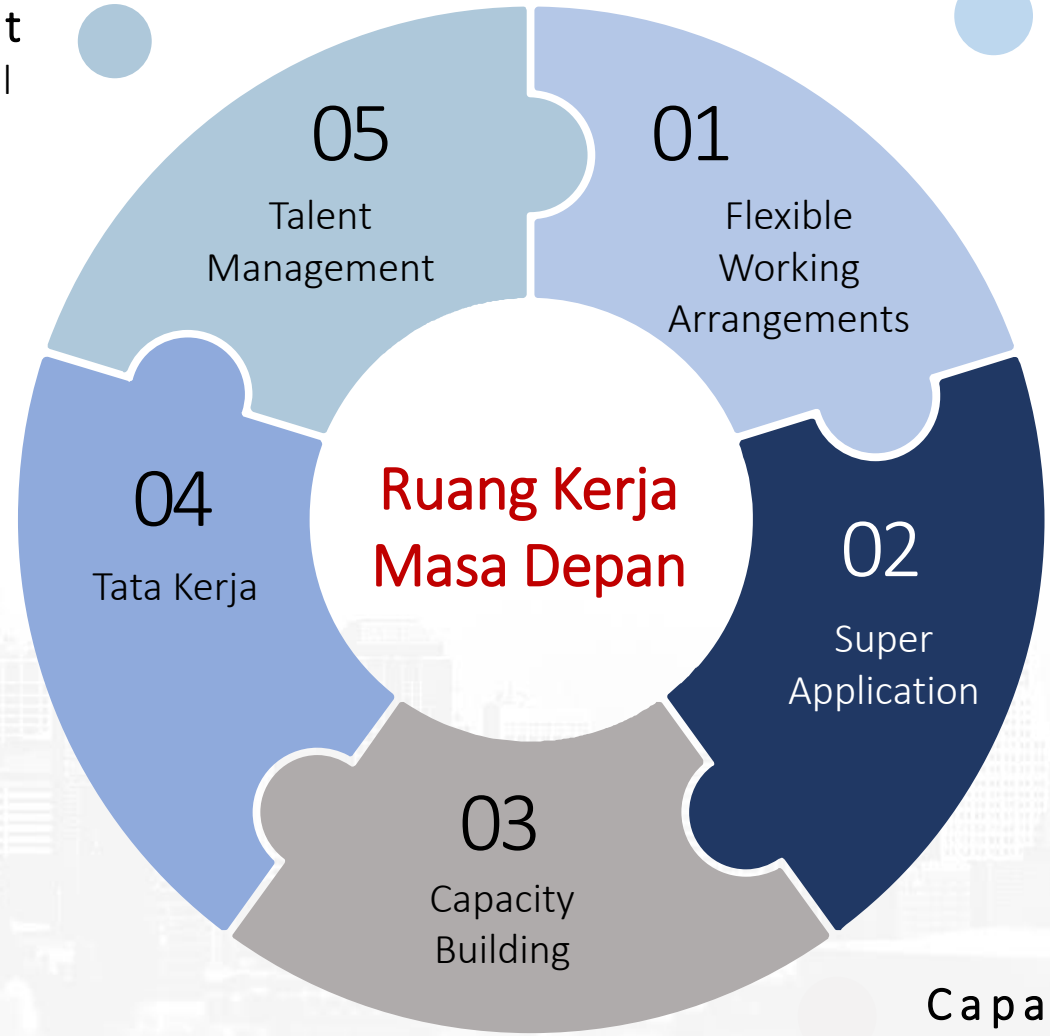
PENCIPTAAN PENGETAHUAN
(Knowledge based Governance)

PERKEMBANGAN GOVERNANSI DUNIA: INDONESIA HARUS MELOMPAT



(Source: Kwon Gi Heon, 2020)

GOVERNANCE 4.0 (DIGITAL GOVERNANCE)



Talent Management

- Sistem karier terbuka nasional (*open career system*)
- Manajemen Talenta Nasional

Flexible Working Arrangements

- *Flexible workspace (co-working space, teleworking)*
- *Flexible work schedule (flexi time)*
- *Squad Team*

Tata Kerja

- Rekayasa proses bisnis (IT-*led reform*)
- Penyederhanaan struktur (*network model*)
- E-Services (smart services)

Super Application

- *Single digital government platform*
- SPBE & RUU Pemerintahan Digital

Capacity Building

- Digital competency ASN
- *Non classical Learning*

TRANSFORMASI DIGITAL DALAM PEMERINTAHAN:
PERAN AI, IOT, DAN BIG DATA

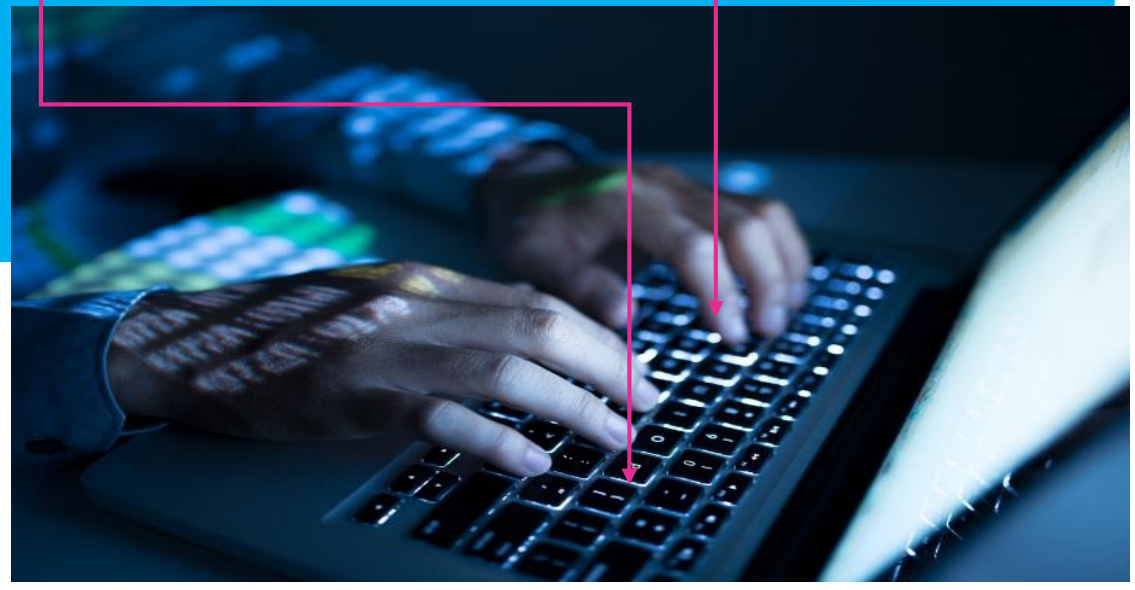
- Algoritma Artificial Intelligence (AI) akan menangani tugas manusia di Administrasi Publik
- “Demokratisasi” Big Data untuk kebijakan dan keputusan strategis
- Internet of Things dapat digunakan layanan publik dan Smart City
- Teknologi akan mebangun perilaku manusia untuk mengurangi stres, menciptakan efisiensi
- Teknologi dan Manusia akan menjadi kolaborator keputusan strategis yang lebih cerdas

Apa itu SMKI dan SPBE ?

Sistem Manajemen Keamanan Informasi (SMKI)
adalah suatu bentuk susunan proses yang dibuat berdasarkan pendekatan resiko bisnis untuk merencanakan (Plan), mengimplementasikan dan mengoperasikan (Do), memonitoring dan meninjau (Check), serta memelihara dan meningkatkan atau mengembangkan (Act) terhadap keamanan informasi perusahaan. Sistem Manajemen Keamanan Informasi biasanya dapat digunakan para manajer untuk mengukur, memonitor dan mengendalikan keamanan informasi. (***ref. ISO 27001:2013***)

Sistem pemerintahan Berbasis Elektronik (SPBE)

Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE
(***Ref. Perpres No. 95 tahun 2018***)



RELEVANSI DAN KETERHUBUNGAN ANTARA STANDAR MANAJEMEN KEAMANAN INFORMASI (SMKI) 27001:2022 DALAM PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

- Sistem Manajemen Keamanan Informasi adalah suatu struktur yang digunakan untuk mengidentifikasi, mengelola, dan melindungi informasi penting dari serangan, kerusakan, dan penyalahgunaan. Sementara Keamanan Sistem Pemerintahan Berbasis Elektronik merupakan suatu struktur yang digunakan oleh pemerintah untuk mengamankan data yang tersimpan di dalam sistemnya.

PDP

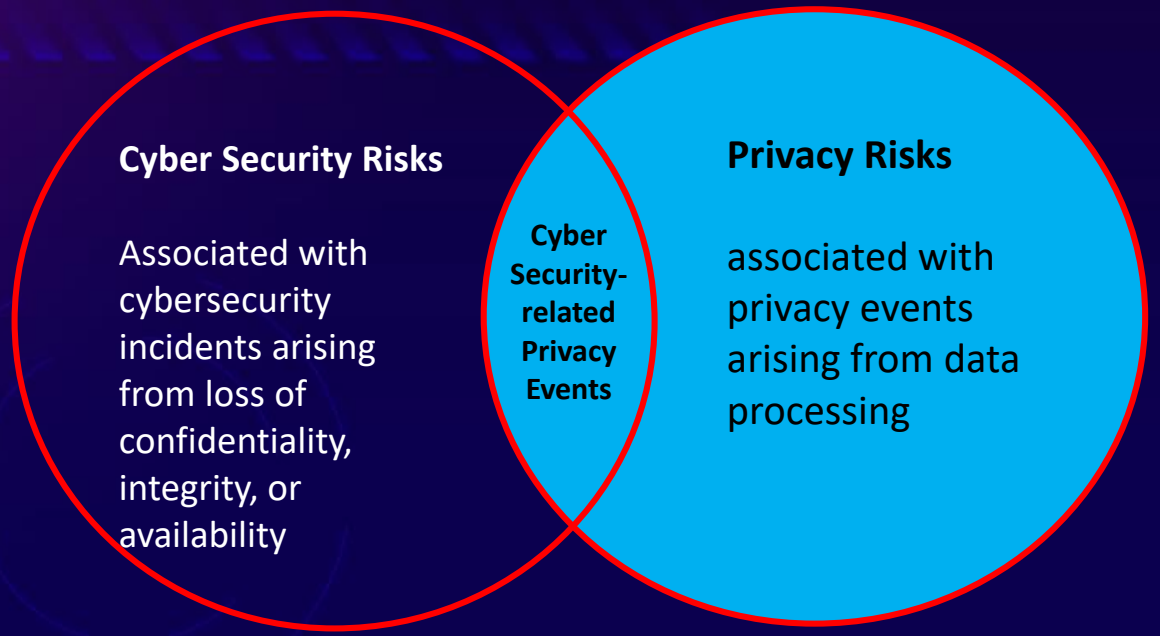
SMKI

SPBE

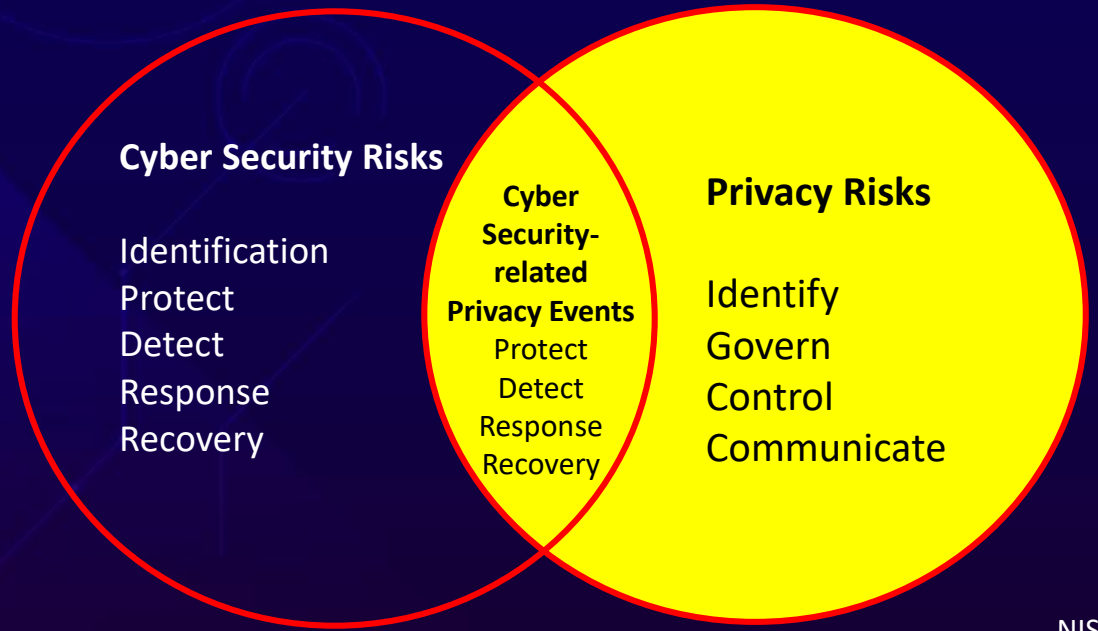
Birokrasi Digital

- Kedua sistem tersebut sangat relevan satu sama lain, karena Sistem Manajemen Keamanan Informasi dapat digunakan untuk melindungi data di dalam sistem pemerintahan berbasis elektronik. Dengan menggunakan Sistem Manajemen Keamanan Informasi, pemerintah dapat mengamankan data pemerintah dari ancaman luar dan memastikan bahwa data tersebut tidak akan disalahgunakan. Selain itu, sistem ini juga dapat digunakan untuk memastikan bahwa sistem pemerintahan berbasis elektronik berjalan dengan baik dan data yang tersimpan tetap terlindungi.

Cybersecurity and Privacy Risk Relationship



Using Functions to Manage Cybersecurity and Privacy Risks



Relationship Between Privacy Risk and Organizational Risk

Problem

Arises from data processing

Individual

experiences direct impact (e.g., embarrassment, discrimination, economic loss)

Organization

resulting impact (e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

Perpres No. 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

UU Adminduk No. 23/2006 dan UU No. 24/2013, terdapat 31 elemen jenis Data Pribadi (dalam diktum UU Adminduk pasal 58);

Penerapan Permendagri 57 thn 2021 tentang Sistem Manajemen Keamanan Informasi Administrasi Kependudukan

NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Januari 2020

Keamanan Informasi Berbagi pakai Data di lingkungan Pemerintah Daerah

Data Interoperability & Security

Data/Informasi didorong untuk mudah diakses dan dibagipakaikan. Hal ini berkaitan dengan mekanisme pemanfaatan Data/Informasi yang mudah namun tetap aman dari kebocoran data, serta cakupan elemen Data yang dibagipakaikan.

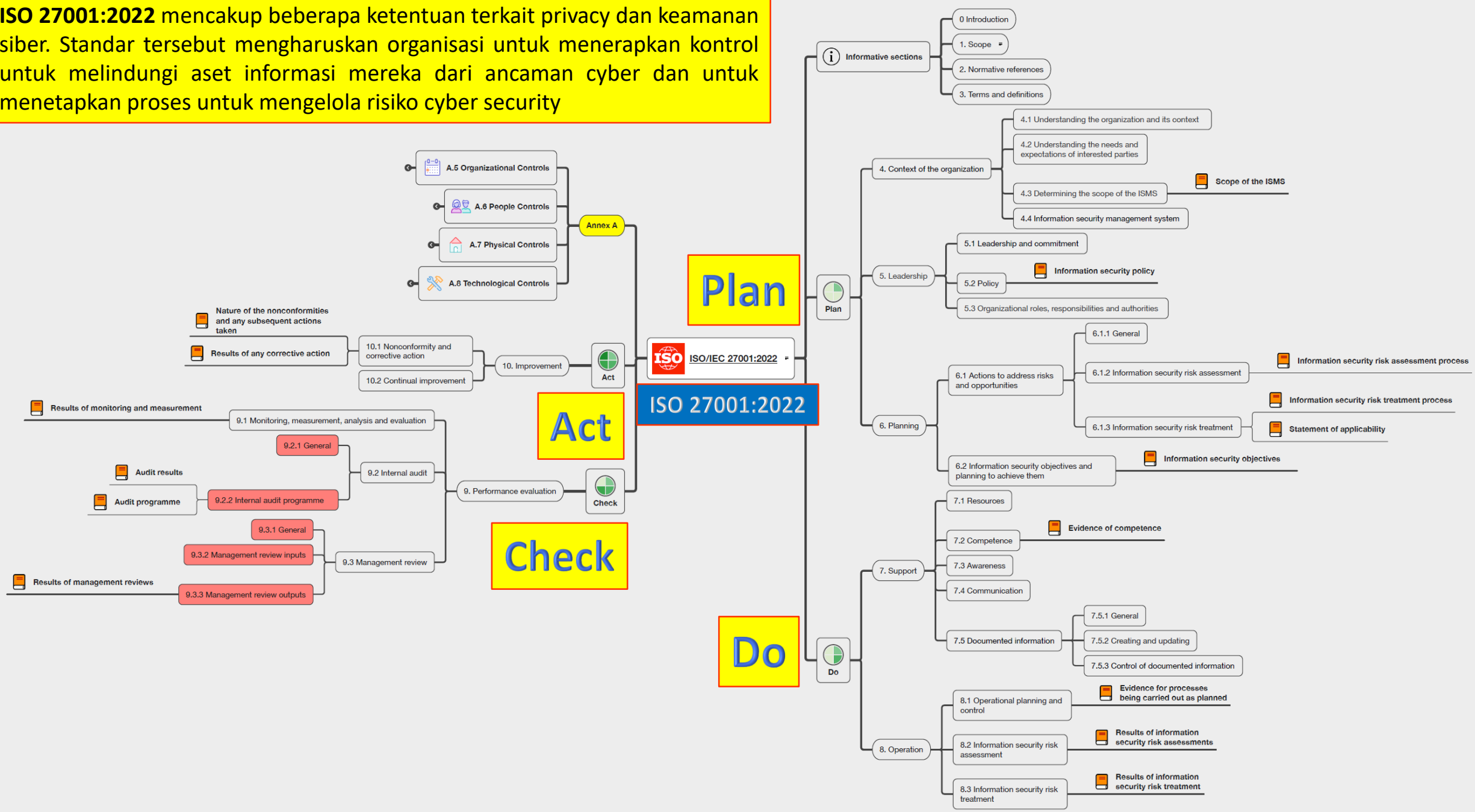
Data Timeliness & Accuracy

Data/Informasi yang dijadikan data induk atau data dasar oleh K/L/D perlu selalu terjaga akurasi dan kemutakhirannya sehingga meningkatkan kualitas pengambilan kebijakan yang dibuat berdasarkan Data/Informasi yang ada

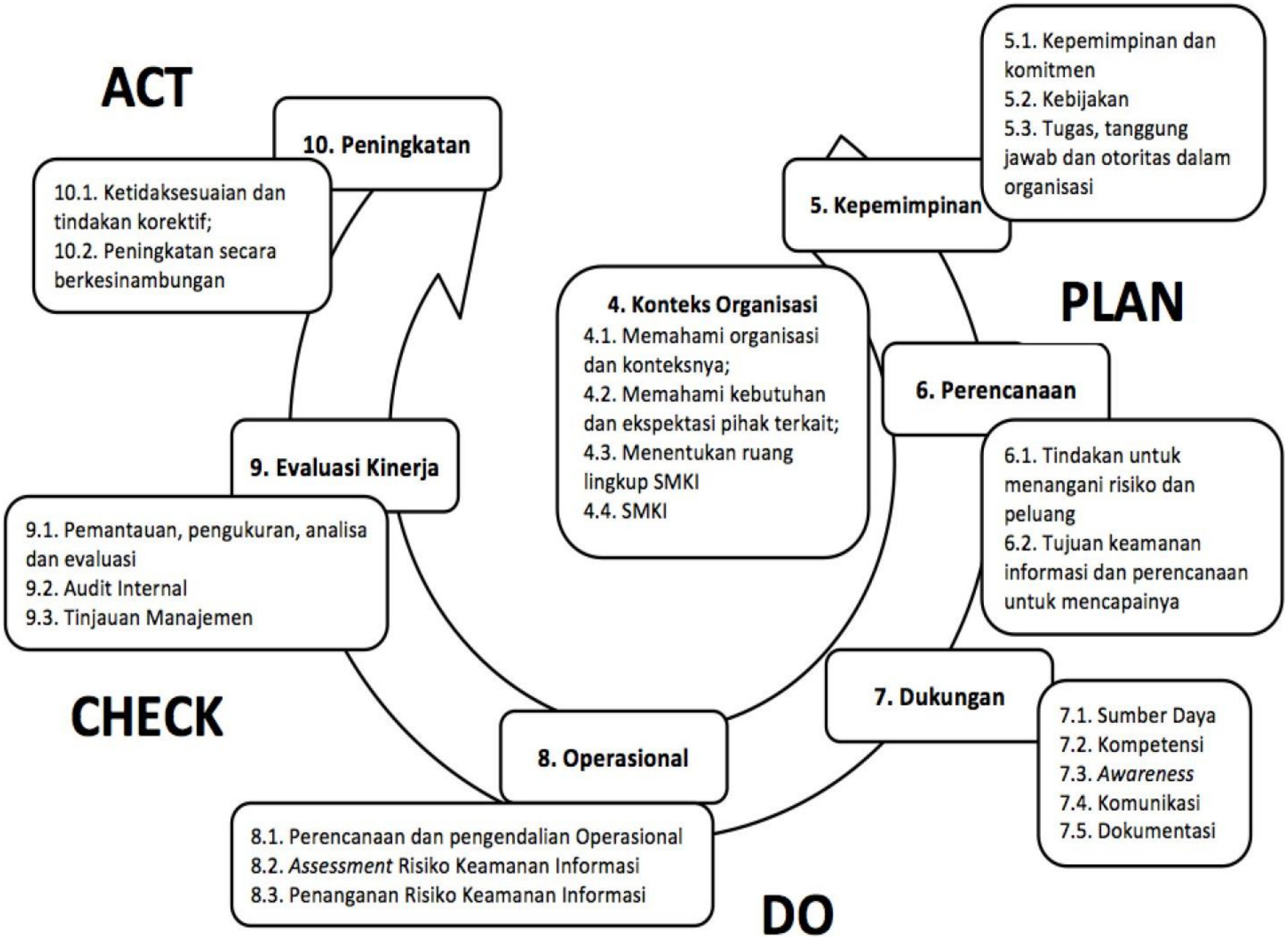
Clear Legal Basis

Diperlukan dasar hukum yang jelas dan kuat untuk memudahkan K/L dalam mengakses Data/Informasi.

ISO 27001:2022 mencakup beberapa ketentuan terkait privacy dan keamanan siber. Standar tersebut mengharuskan organisasi untuk menerapkan kontrol untuk melindungi aset informasi mereka dari ancaman cyber dan untuk menetapkan proses untuk mengelola risiko cyber security



Struktur SNI/ ISO 27001:2013



27001 : 2013 control	27001 : 2022 control
A.18.1.4 Privacy and protection of personal information	A.5.34 Privacy and protection of personal identifiable information (PII)
NEW	A.5.7 Threat intelligence
NEW	A.7.4 Physical security monitoring
NEW	A.8.16 Monitoring activities
NEW	A.8.9 Configuration management
NEW	A.8.10 Information deletion
NEW	A.8.11 Data masking
NEW	A.8.12 Data leakage prevention
NEW	A.8.22 Web filtering
NEW	A.8.28 Secure coding
NEW	A.5.23 Information security for use of cloud services
NEW	A.5.30 ICT readiness for business continuity

BSSN dalam Keamanan Sistem Elektronik Tranformasi Digital di Indonesia

TIM KOORDINASI SPBE NASIONAL
PERAN DALAM PENERAPAN ARSITEKTUR SPBE

Peraturan Presiden No. 132/2022

Menteri PANRB

- **Ketua Tim Koordinasi SPBE Nasional (*Chief Information Officer* – CIO Nasional)**
- Mengoordinasikan seluruh program SPBE Nasional (Project Managemen Office – PMO Nasional)
- Mengoordinasikan **keselarasan Arsitektur SPBE Instansi Pemerintah**
- **Pembina Domain Arsitektur Proses Bisnis**
- **Pembina Domain Layanan SPBE**

Menteri PPN/ Bappenas

- Mengoordinasikan perencanaan SPBE K/L dan Nasional, sesuai Arsitektur SPBE Nasional
- **Pembina Domain Arsitektur Data dan Informasi** (Selaras dengan Kerangka Satu Data Indonesia)
- **Chief Data Officer (CDO) Nasional**

SATU DATA INDONESIA

Menteri Keuangan

- Mengoordinasikan penganggaran SPBE K/L dan Nasional, sesuai Arsitektur SPBE Nasional
- **Chief Financial Officer (CFO) Nasional**

Kepala BSSN

- Menyusun standar keamanan SPBE Nasional
- Mengkoordinasikan dan Asistensi Penerapan Standar Keamanan SPBE
- Menetapkan manajemen dan melaksanakan audit keamanan SPBE
- **Pembina Domain Arsitektur Keamanan SPBE**
- **Chief Information Security Officer (CISO) Nasional**

Menteri Kominfo

- **Pembina Domain Arsitektur Aplikasi**
- **Pembina Domain Arsitektur Infrastruktur SPBE**
- **Chief Technology Officer (CTO) Nasional**

Menteri Dalam Negeri

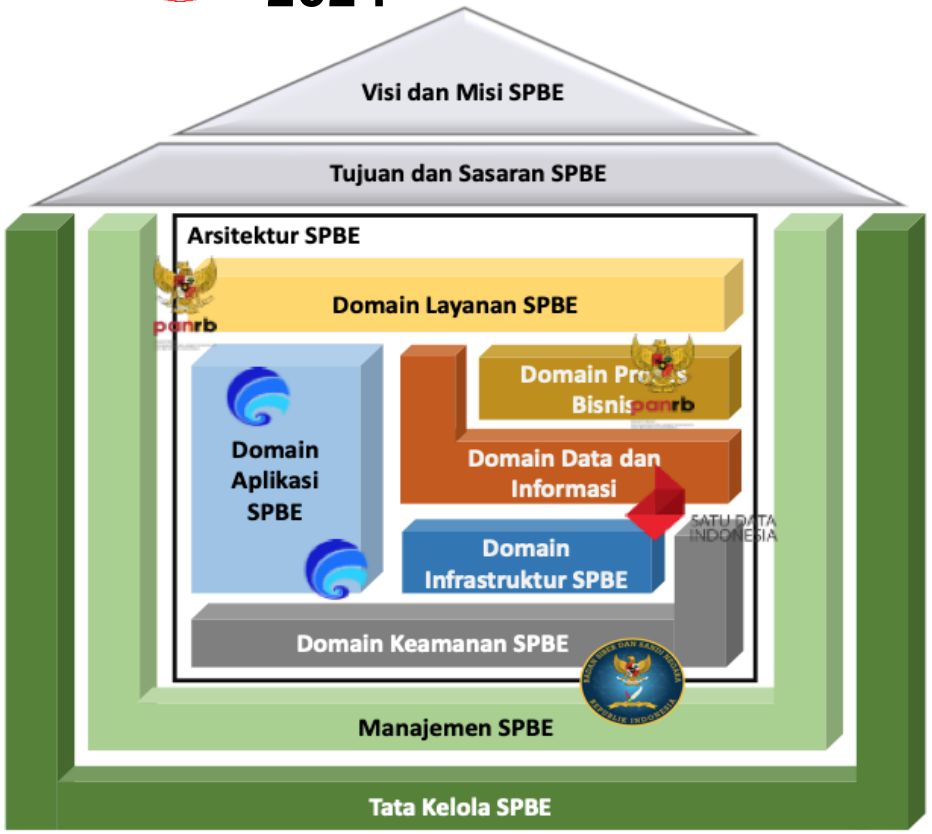
- Mengoordinasikan penerapan SPBE di Pemda, melalui pemanfaatan Arsitektur SPBE
- Mendorong komitmen Kepala Daerah, untuk menyusun dan menetapkan Arsitektur SPBE Pemerintah Daerah selaras dengan Arsitektur SPBE Nasional
- **Chief Regional Government Officer (CRGO)**

Kepala BRIN

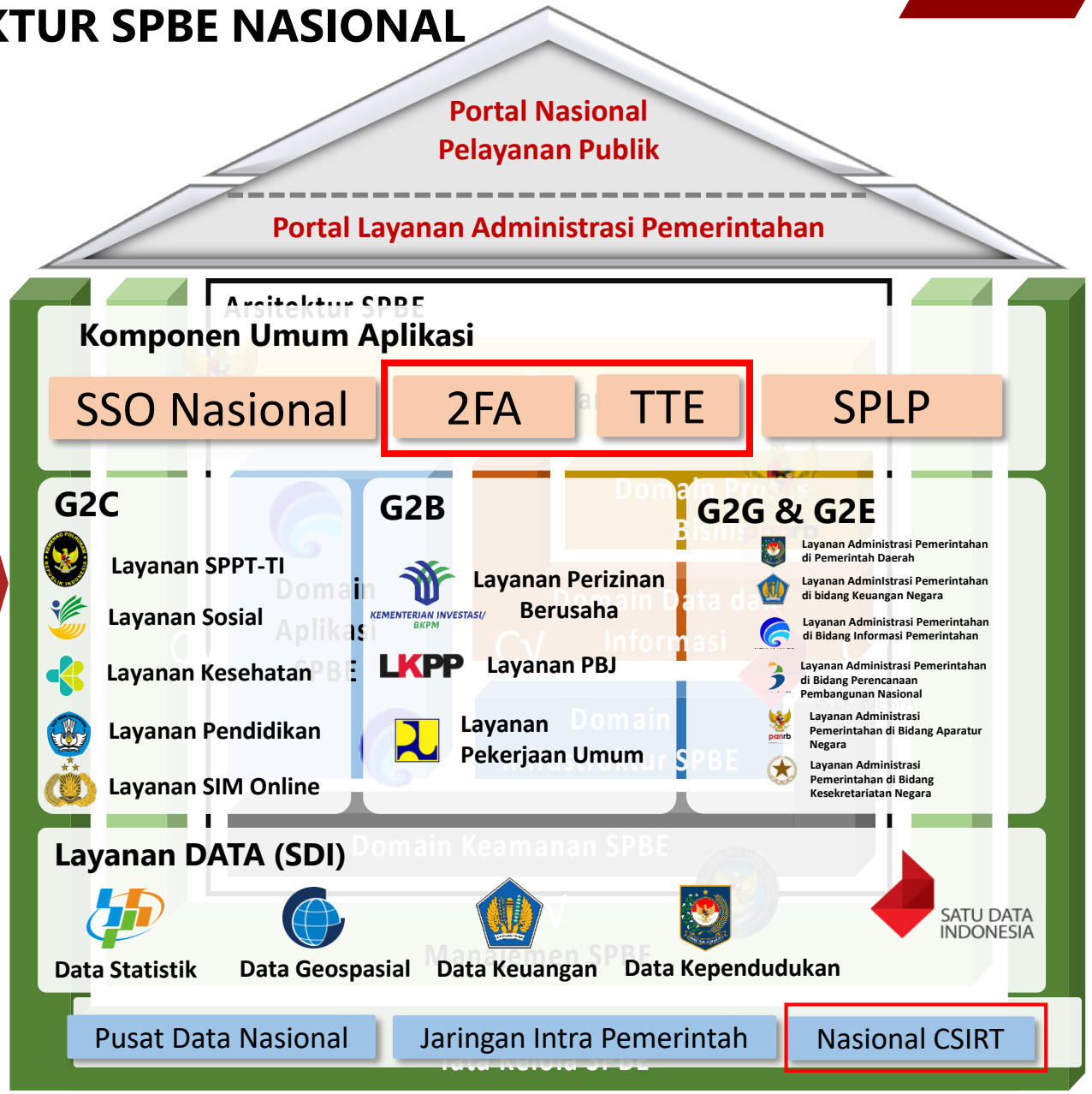
- Pemanfaatan Arsitektur SPBE dalam pelaksanaan riset dan menciptakan inovasi layanan digital, seperti penggunaan kecerdasan artifisial
- **Chief Research and Innovation Officer (CRIO) Nasional**

** Gambar diambil dari Paparan KemenpanRB terkait Inisiatif Strategis Arsitektur SPBE Nasional*

QUICK WINS PROGRAM BSSN TERHADAP INISIATIF STRATEGIS TARGET ARSITEKTUR SPBE NASIONAL 2024



Inisiatif Strategis 2024



Berdasarkan Desain Inisiatif Strategis, BSSN dapat berkontribusi pada 3 (Tiga) Quick Wins (Program Utama) Keamanan :

1. ***Program Pemenuhan Sertifikat Elektronik untuk mendukung Penerapan Tanda Tangan Elektronik (TTE);***
2. ***Program Asistensi Penerapan Standar Keamanan SPBE dan Memberikan Rekomendasi Kelaikan Keamanan (ITSA & Hardening System); dan***
3. ***Audit Keamanan Aplikasi Umum dan Infrastruktur SPBE Nasional.***

**** Gambar diambil dari Paparan KemenpanRB terkait Inisiatif Strategis Arsitektur SPBE Nasional***

BSSN DALAM MENDUKUNG SPBE NASIONAL*

ARSITEKTUR

Bersama Kemenpan RB terkait Penetapan Arsitektur SPBE Nasional (BSSN Domain Keamanan SPBE)

PASAL 9 (3)

KEAMANAN

- Penetapan Standar teknis dan prosedur keamanan SPBE ;
- **Asistensi** Penerapan keamanan dan Asistensi penyelesaian; permasalahan keamanan SPBE.

Pasal 41

MANAJEMEN

Penetapan Pedoman manajemen keamanan Informasi SPBE & Memberikan Asistensi Penerapan Manajemen Keamanan Informasi SPBE

PASAL 48

INFRASTRUKTUR

Memberikan Rekomendasi Kelaikan Keamanan pada PDN, JIP & SPLP

Pasal 30, 32, 33

AUDIT

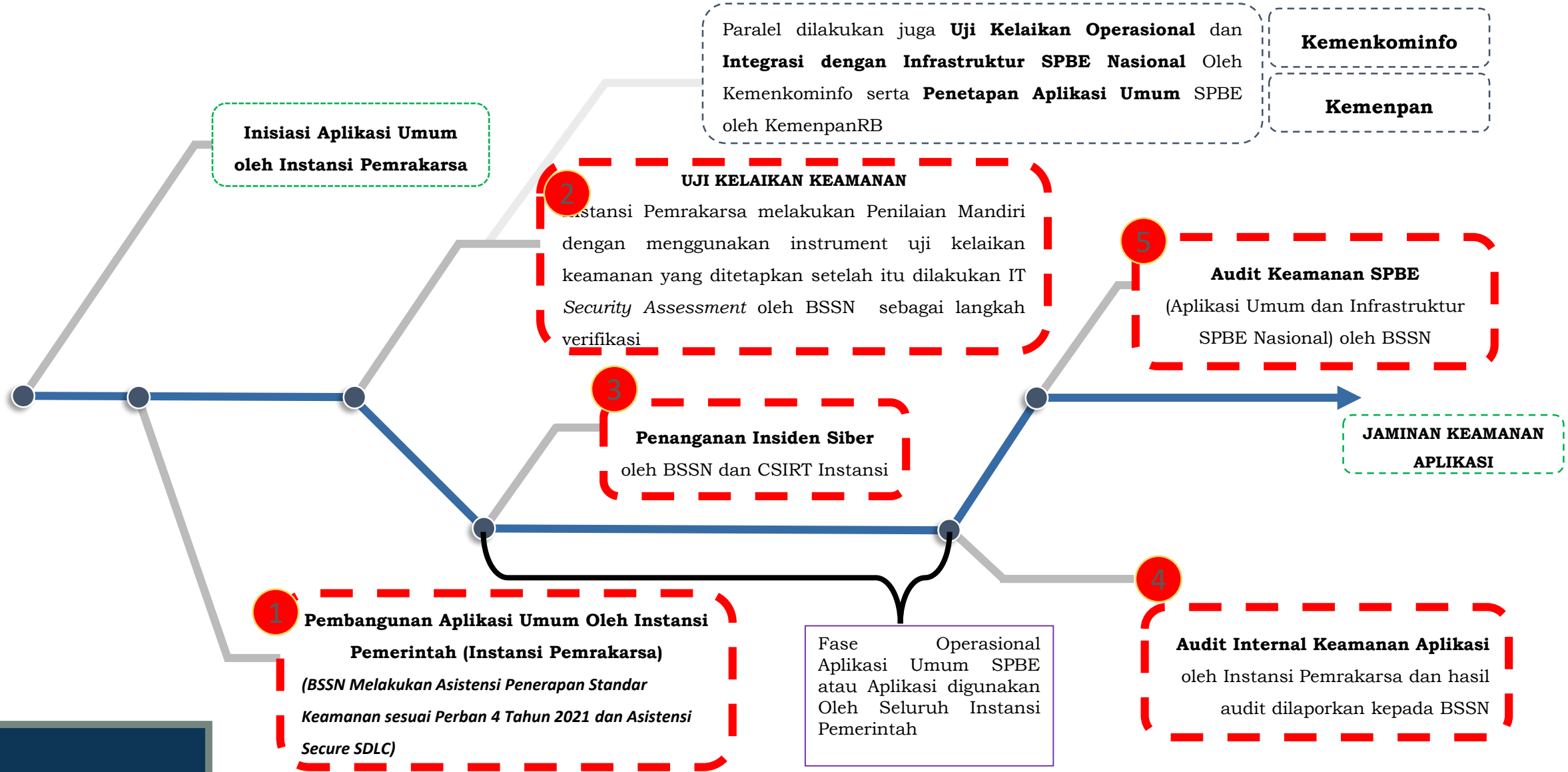
- Penetapan Standar dan Tatacara Audit Keamanan SPBE;
- Pelaksanaan Audit Keamanan Aplikasi Umum dan Infrastruktur SPBE Nasional;
- Sebagai Latik Pemerintah.

Pasal 58

* Sesuai dengan Perpres 95/2018 tentang SPBE

BADAN SIBER DAN SANDI NEGARA

SIKLUS PERAN BSSN DALAM MENDUKUNG KEAMANAN APLIKASI UMUM SPBE TAHUN 2023-2025



PENDEKATAN TEKNIS BSSN
DALAM SIKLUS KEAMANAN APLIKASI UMUM SPBE/INTEGRASI APLIKASI TAHUN 2023-2025

Tahap Inisiasi Saat Pembangunan dan pengembangan Aplikasi

1. Asistensi Penerapan Standar Teknis dan Prosedur Keamanan SPBE dengan mengacu terhadap Perban No. 4 tahun 2021;
2. Asistensi Secure SDLC (Software Development Life Cycle) pada tahap Pengembangan Aplikasi Umum SPBE.

Tahap Pasca Inisiasi Saat Aplikasi telah selesai dibangun/dikembangkan

3. Pemberian Rekomendasi Kelaikan Keamanan melalui Metode IT *Security Assessment* (Identifikasi Kerentanan) dan *Hardening System* (Perbaikan Kerentanan dan Peningkatan Keamanan).

Tahap Operasional Selama Aplikasi Beroperasi/Digunakan

4. Secure Hosting dan Monitoring NSOC Aplikasi Umum SPBE;
5. Penanganan Insiden melalui Tim CSIRT Nasional dan CSIRT Instansi.

Tahap Evaluasi Setelah 1 Tahun Aplikasi Digunakan

6. Audit Keamanan Aplikasi Umum SPBE dan Infrastruktur SPBE Nasional;
7. Pemeliharaan dan Evaluasi Penerapan Sertifikat Elektronik.

Asistensi Penerapan Standar Keamanan Aplikasi

Pembangunan Aplikasi oleh Instansi Harus Menerapkan standar keamanan yang ditetapkan dalam Perban BSSN No 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE

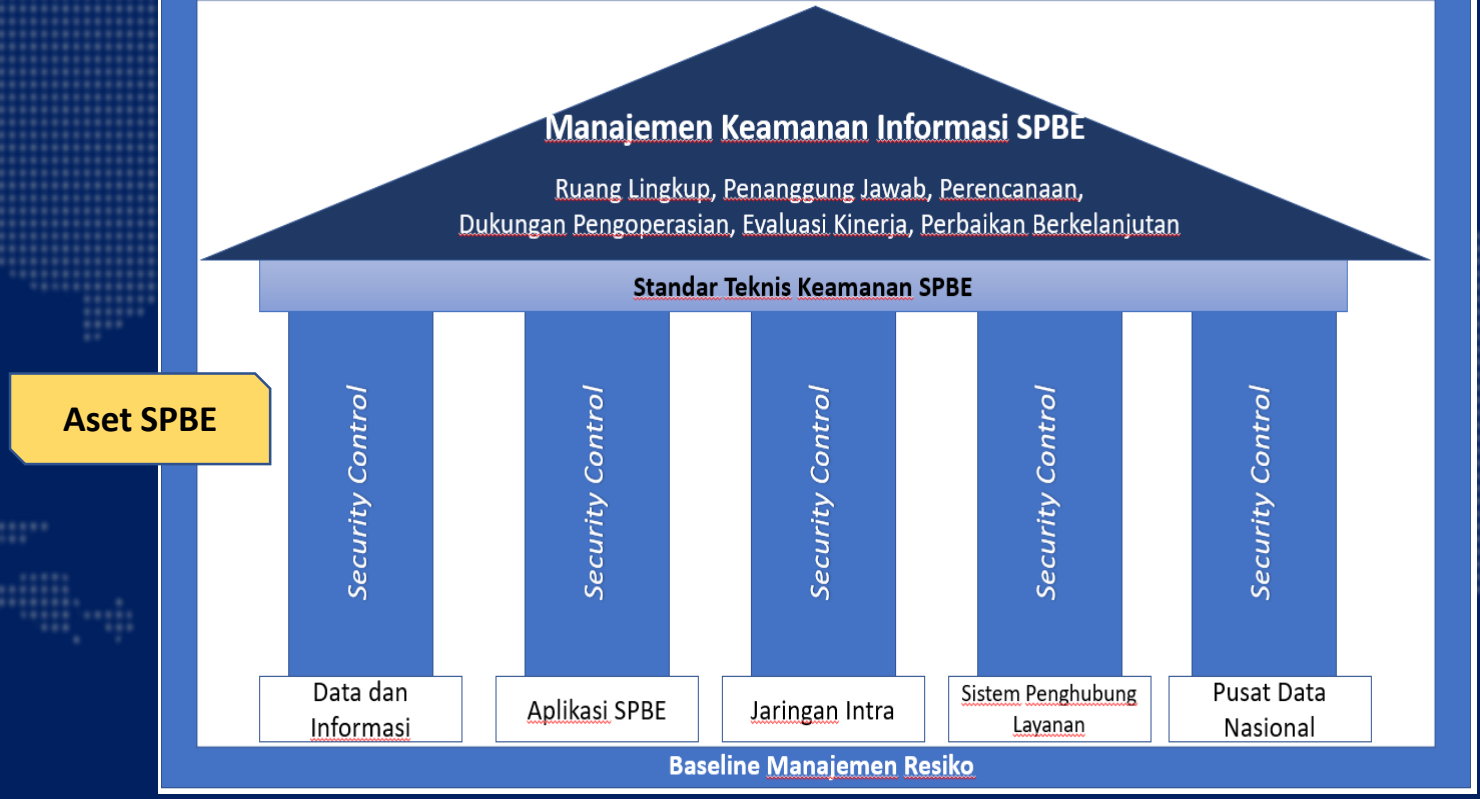
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 4 TAHUN 2021
TENTANG
PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

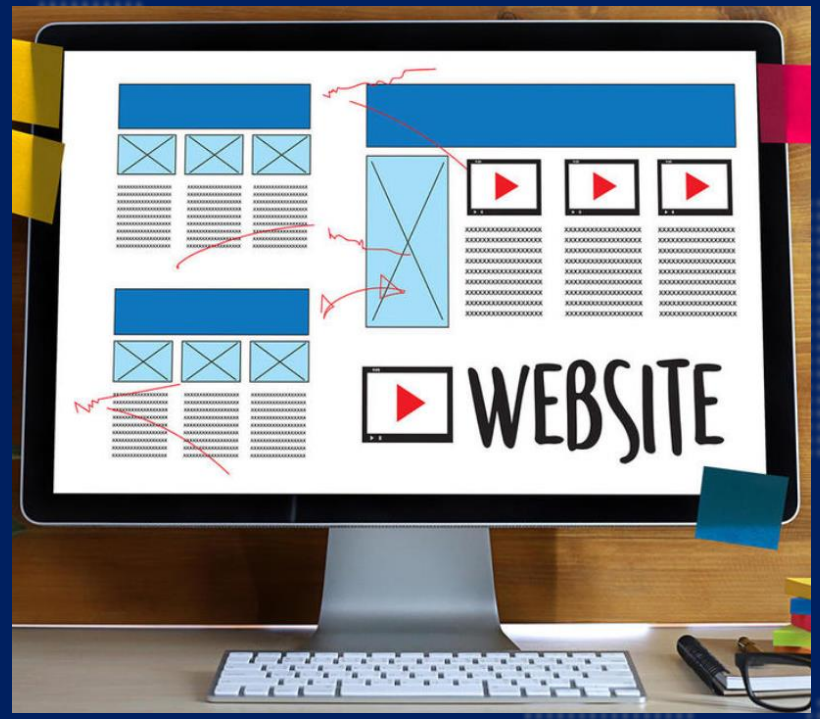
Menimbang : bahwa untuk melaksanakan ketentuan Pasal 41 ayat (4) dan Pasal 48 ayat (5) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur 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 2 Tahun 2018 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2018 Nomor 197);



Keamanan Aplikasi SPBE

Standar Teknis Keamanan Aplikasi SPBE Berbasis WEB



Perban 4 Th 2021 Pasal 26:

- Autentikasi
- Manajemen Sesi
- Persyaratan Kontrol Akses
- Validasi Input
- Kriptografi pada verifikasi statis
- Penanganan eror dan pencatatan log
- Proteksi Data
- Keamanan Komunikasi
- Pengendalian kode berbahaya
- Logika bisnis
- File
- Keamanan API dan Web Service
- Keamanan Konfigurasi

Keamanan Aplikasi SPBE

Standar Teknis Keamanan Aplikasi SPBE Berbasis Mobile

Perban 4 Th 2021 Pasal 28:

- Penyimpanan data dan persyaratan privasi
- Kriptografi
- Autentikasi dan Manajemen Sesi
- Komunikasi Jaringan
- Interaksi Platform
- Kualitas kode dan Pengaturan *build*
- Ketahanan

PENERAPAN SMKI DALAM PENYELENGGARAAN SPBE DI PEMERINTAH PROVINSI JAWA TENGAH

MENTERI
PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA

KEPUTUSAN
MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA
NOMOR 108 TAHUN 2023
TENTANG
HASIL PEMANTAUAN DAN EVALUASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PADA INSTANSI PUSAT DAN PEMERINTAH DAERAH
TAHUN 2022

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA,

Menimbang :

a. bahwa untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya melalui penerapan sistem pemerintahan berbasis elektronik pada instansi pusat dan pemerintah daerah, dilakukan kegiatan pemantauan dan evaluasi sistem pemerintahan berbasis elektronik Tahun 2022;

b. bahwa berdasarkan hasil pemantauan dan evaluasi tersebut di atas, telah diperoleh nilai indeks dan predikat sistem pemerintahan berbasis elektronik pada instansi pusat dan pemerintah daerah tahun 2022; dan

c. berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi tentang Hasil Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik pada Instansi Pusat dan Pemerintah Daerah Tahun 2022;

INDEKS SPBE 2022

Hasil Pemantauan SPBE Pemerintah Daerah di Jawa Tengah

No	Nama Instansi	Indeks	Predikat
1	Pemerintah Provinsi Jawa Tengah	3,34	Baik
2	Pemerintah Kab. Semarang	2,13	Cukup
3	Pemerintah Kab. Kendal	2,93	Baik
4	Pemerintah Kab. Grobogan	3,37	Baik
5	Pemerintah Kab. Pekalongan	2,62	Baik
6	Pemerintah Kab. Batang	2,85	Baik
7	Pemerintah Kab. Tegal	3,07	Baik
8	Pemerintah Kab. Brebes	2,40	Cukup
9	Pemerintah Kab. Kudus	3,38	Baik
10	Pemerintah Kab. Pemalang	2,23	Cukup
11	Pemerintah Kab. Jepara	3,14	Baik
12	Pemerintah Kab. Rembang	3,19	Baik
13	Pemerintah Kab. Blora	2,36	Cukup
14	Pemerintah Kab. Banyumas	2,60	Baik
15	Pemerintah Kab. Cilacap	2,87	Baik
16	Pemerintah Kab. Purbalingga	3,20	Baik
17	Pemerintah Kab. Banjarnegara	2,86	Baik
18	Pemerintah Kab. Magelang	3,13	Baik
19	Pemerintah Kab. Wonosobo	2,90	Baik
20	Pemerintah Kab. Purworejo	2,80	Baik
21	Pemerintah Kab. Kebumen	3,44	Baik
22	Pemerintah Kab. Sragen	3,10	Baik
23	Pemerintah Kab. Sukoharjo	3,42	Baik
24	Pemerintah Kab. Karanganyar	3,32	Baik
25	Pemerintah Kab. Wonogiri	3,34	Baik
26	Pemerintah Kota Semarang	3,38	Baik
27	Pemerintah Kota Salatiga	2,84	Baik
28	Pemerintah Kota Tegal	3,05	Baik
29	Pemerintah Kota Magelang	2,67	Baik
30	Pemerintah Kota Surakarta	3,73	Sangat Baik

UU No. 23 tahun 2014 tentang Pemda	Persandian untuk pengamanan informasi, urusan pemerintahan bidang persandian halaman 88
Perpres No. 95 tahun 2018 tentang SPBE	Pasal 6 → Arsitektur SPBE Pemda Pasal 19 → Peta Rencana SPBE Pemerintah Daerah disusun dengan berpedoman pada Peta Rencana SPBE Nasional. Pasal 22 → Pemda menyusun rencana anggaran Pasal 27 → Infrastruktur SPBE Pemda
Perpres No. 39 tahun 2019 tentang SDI	Pasal 21 → Setiap Pemerintah Daerah hanya menriliki 1 (satu) Instansi Daerah yang meiaksanakan tugas Walidata tingkat daerah.
Perpres No. 132 tahun 2022 tentang Arsitektur SPBE	Pasal 3, (5) Kepala daerah menetapkan Arsitektur SPBE Pemerintah Daerah dengan keputusan kepala daerah paling lambat tahun 2023.

Perpres 95 Tahun 2018

Sistem Pemerintahan Berbasis Elektronik

SALINAN

PRESIDEN
REPUBLIK INDONESIA

PERATURAN PRESIDEN REPUBLIK INDONESIA

NOMOR 95 TAHUN 2018

TENTANG

SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya diperlukan sistem pemerintahan berbasis elektronik;

Amanat Pelaksanaan Keamanan Informasi

Pasal 41

(1) Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan SPBE.

(2) Dalam menerapkan Keamanan SPBE dan menyelesaikan permasalahan Keamanan SPBE, pimpinan Instansi Pusat dan kepala daerah dapat melakukan konsultasi dan/atau koordinasi dengan kepala lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

(3) Penerapan Keamanan SPBE harus memenuhi standar teknis dan prosedur Keamanan SPBE.

(4) Ketentuan lebih lanjut mengenai standar teknis dan prosedur Keamanan SPBE diatur dengan Peraturan Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Manajemen Keamanan Informasi

Bagian Ketiga

Manajemen Keamanan Informasi

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.

SALINAN

PRESIDEN
REPUBLIK INDONESIA

PERATURAN PRESIDEN REPUBLIK INDONESIA

NOMOR 132 TAHUN 2022

TENTANG

ARSITEKTUR SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK NASIONAL

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 9 ayat (4) dan Pasal 74 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Presiden tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional;

Mengingat :

1. Pasal 4 ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
3. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);

MEMUTUSKAN:

Menetapkan : PERATURAN PRESIDEN TENTANG ARSITEKTUR SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK NASIONAL.

Pasal 1

Dalam Peraturan Presiden ini yang dimaksud dengan:

1. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.

2. Arsitektur . . .

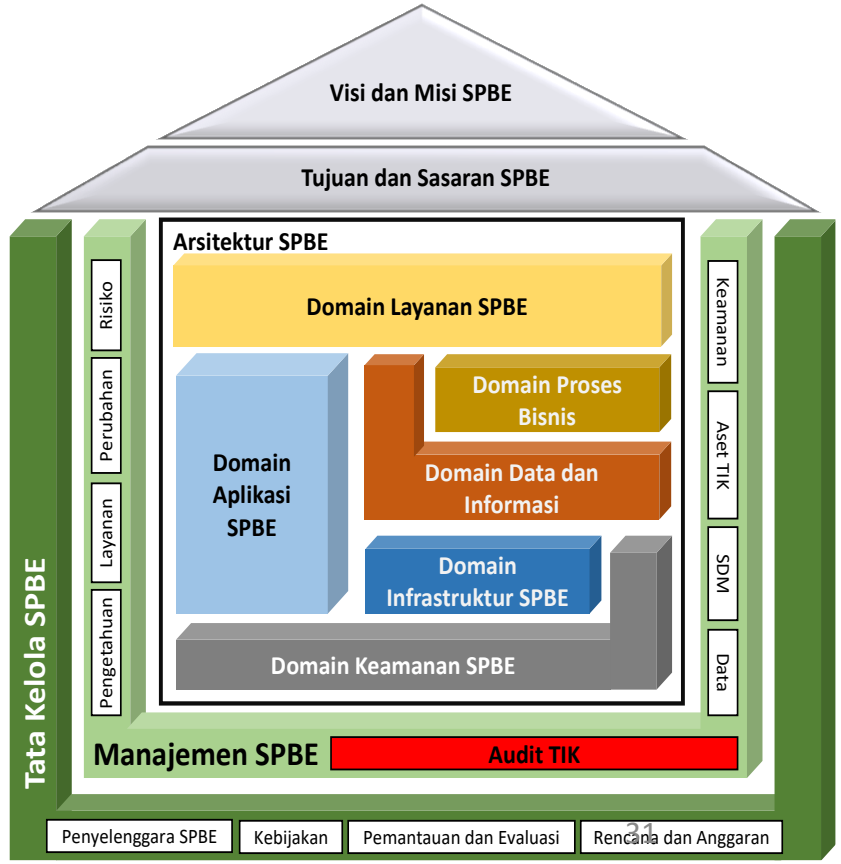
Perpres No 132 Tahun 2022 tentang Arsitektur SPBE Nasional

Perpres Arsitektur SPBE Merupakan Amanat dari Pasal 9 Perpres Nomor 95 Tahun 2018 tentang SPBE.

Arsitektur SPBE adalah **kerangka dasar yang mendeskripsikan integrasi antar domain :**

1. Proses bisnis,
2. Layanan
3. Data dan informasi,
4. Infrastruktur SPBE,
5. Aplikasi SPBE, dan
6. Keamanan SPBE

Pasal 3, (5) Kepala daerah menetapkan Arsitektur SPBE Pemerintah Daerah dengan keputusan kepala daerah paling lambat tahun 2023.



PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 4 TAHUN 2021
TENTANG
PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

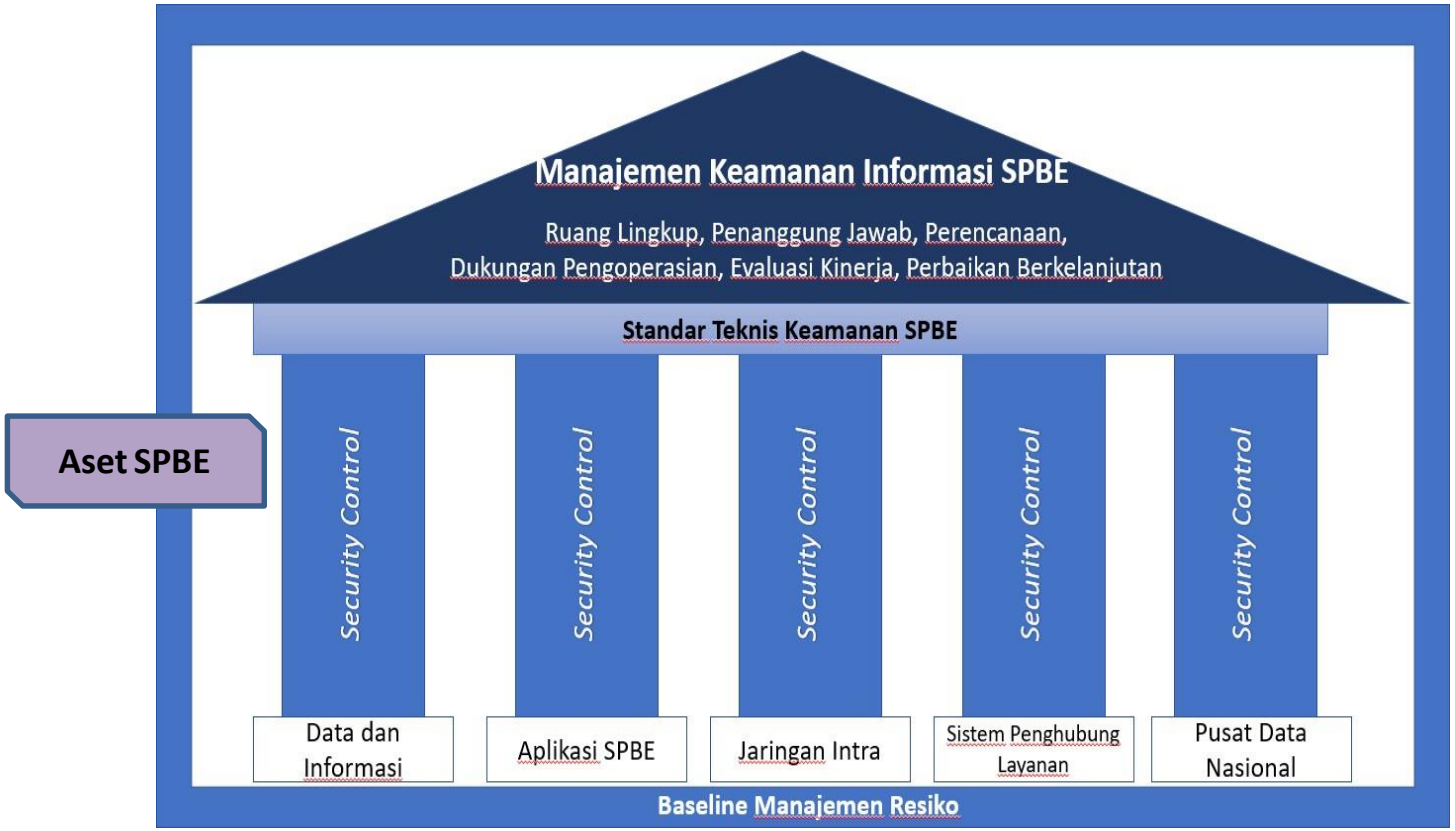
Menimbang : bahwa untuk melaksanakan ketentuan Pasal 41 ayat (4) dan Pasal 48 ayat (5) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur 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 2 Tahun 2018 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2018 Nomor 197);

Peraturan BSSN No 4 Tahun 2021

Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE

Perban BSSN No.4 Tahun 2021 Merupakan Amanat dari Pasal 41 dan Pasal 48 Perpres Nomor 95 Tahun 2018 tentang SPBE.



Pedoman Manajemen Keamanan Informasi

Pasal 3

(1) Pedoman manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 merupakan acuan dalam melaksanakan serangkaian proses manajemen keamanan informasi yang meliputi:
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;
   c. perencanaan;
   d. dukungan pengoperasian;
   e. evaluasi kinerja; dan
   f. perbaikan berkelanjutan.

(2) Proses sebagaimana dimaksud pada ayat (1) ditetapkan oleh setiap pimpinan Instansi Pusat dan kepala daerah.

(3) Instansi Pusat dan Pemerintah Daerah mengomunikasikan dan mendokumentasikan kegiatan manajemen keamanan informasi SPBE masing-masing.

Penanggung jawab dan pelaksana SMPI

Pasal 5

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b dilaksanakan oleh pimpinan Instansi Pusat dan kepala daerah.

(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh sekretaris Instansi Pusat dan sekretaris daerah pada Pemerintah Daerah.

(3) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, sekretaris Instansi Pusat dan sekretaris daerah pada Pemerintah Daerah disebut sebagai koordinator SPBE.

Pasal 6

(1) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (3) menetapkan pelaksana teknis Keamanan SPBE.

(2) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:

a. pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi pada Instansi Pusat dan Pemerintah Daerah masing-masing; dan

b. pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE.

Permenpan No. 59 Tahun 2020

Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik

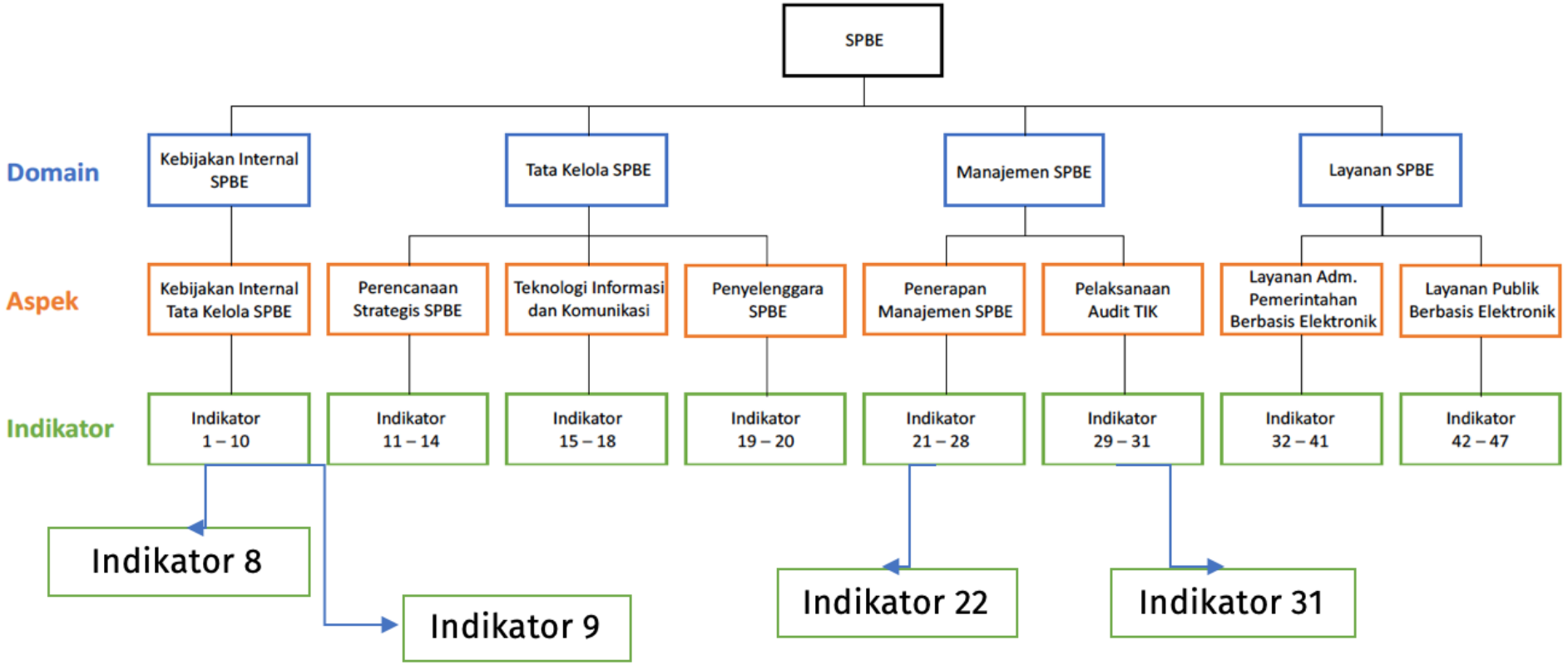
SALINAN

MENTERI
PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA

PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA
NOMOR 59 TAHUN 2020
TENTANG
PEMANTAUAN DAN EVALUASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA,



Indikator Keamanan yang dinilai adalah terkait manajemen keamanan informasi dan audit keamanan SPBE, indikator keamanan tersebut masuk pada :

a. Indikator 8 : tingkat kematangan kebijakan internal manajemen keamanan informasi
b. Indikator 9 : Tingkat Kematangan Kebijakan Internal Audit TIK
c. Indikator 22 : Tingkat Kematangan Penerapan Manajemen Keamanan Informasi
d. Indikator 31 : Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

Tingkat Kematangan Kebijakan Internal Manajemen Keamanan Informasi

Apakah Instansi Pusat/Pemerintah Daerah memiliki kebijakan internal Manajemen Keamanan Informasi?

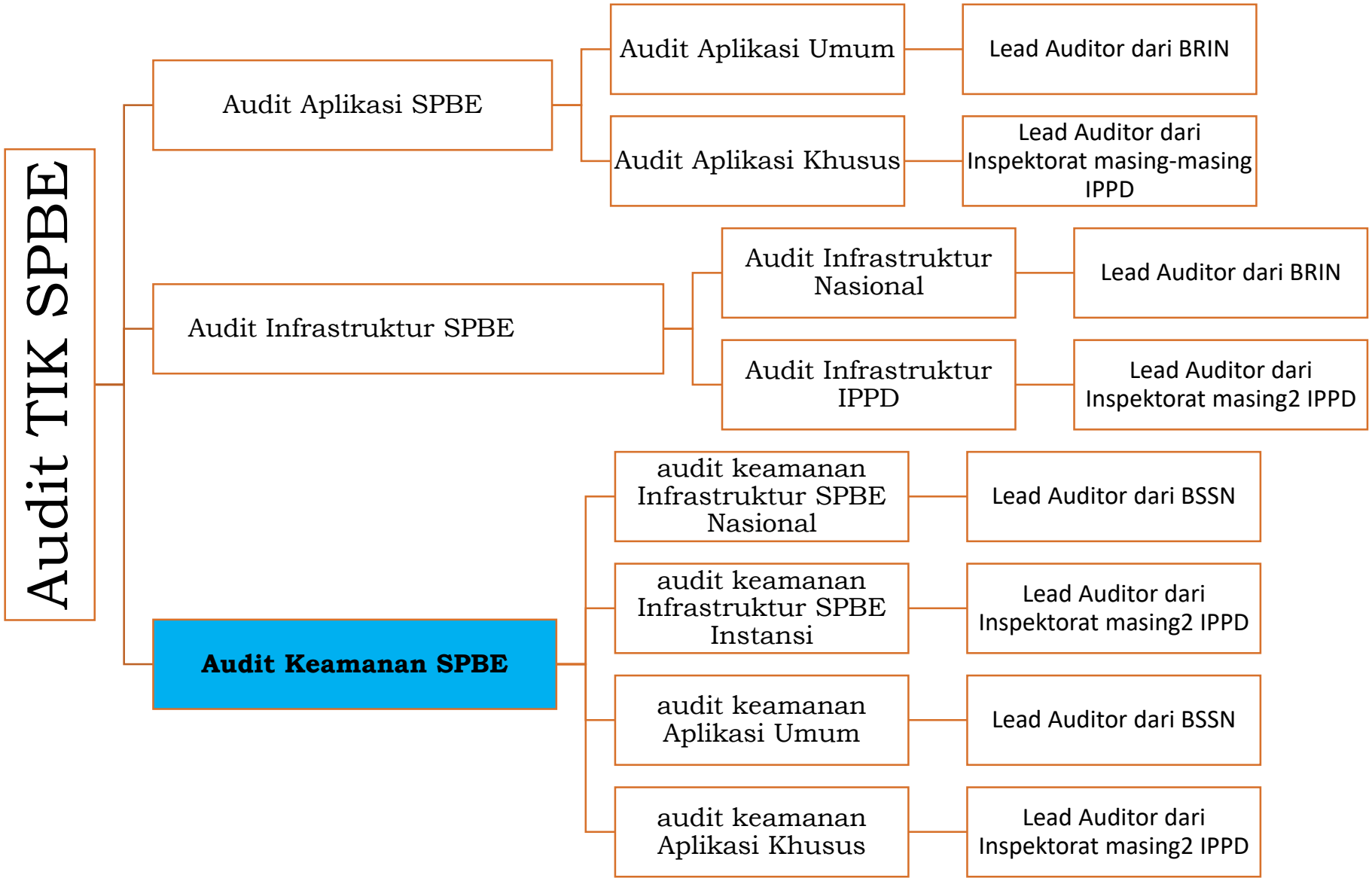
Tingkat	Kriteria
1	Konsep kebijakan internal terkait Manajemen Keamanan Informasi belum atau telah tersedia.
2	Kebijakan internal terkait Manajemen Keamanan Informasi telah ditetapkan. Kondisi: Kebijakan internal terkait Manajemen Keamanan Informasi belum mengatur secara lengkap mengenai cakupan Manajemen Keamanan Informasi (penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan Informasi).
3	Kriteria tingkat 2 telah terpenuhi dan kebijakan internal terkait Manajemen Keamanan Informasi mengatur seluruh cakupan Manajemen Keamanan Informasi secara lengkap (**penetapan ruang lingkup**, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan Informasi).
4	Kriteria tingkat 3 telah terpenuhi, dan kebijakan internal terkait Manajemen Keamanan Informasi telah mengatur penerapan untuk seluruh unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah. Selain itu, kebijakan internal terkait Manajemen Keamanan Informasi telah direviu dan dievaluasi secara periodik.
5	Kriteria tingkat 4 telah terpenuhi serta hasil reviu dan evaluasi kebijakan internal terkait Manajemen Keamanan Informasi telah ditindaklanjuti dengan kebijakan baru.

Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

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.

TORPOLOGI/SEGMENTASI AUDIT TIK SPBE



KETERANGAN :

- Lead Auditor dapat bekerjasama dengan LATIK (Lembaga Audit TIK) dari pihak swasta terakreditasi atau LAKI (Lembaga Audit Keamanan Informasi);
- Lead Auditor dari Inspektorat masing-masing IPPD selain dapat bekerjasama dengan LATIK/LAKI, Inspektorat dapat bekerjasama dengan personil Diskominfo atau Dinas lainnya untuk terlibat dalam Tim Audit, selama Dinas tersebut tidak menjadi area yang dilakukan audit

Permendagri Nomor 18 tahun 2020
Peraturan Pelaksanaan Peraturan Pemerintah no 13 tahun 2019 tentang Laporan dan Evaluasi Penyelenggaraan Pemerintah Daerah

Konsep/Definisi	:	Mengukur tingkat keamanan informasi pemerintah
Rumus	:	$\frac{Jumlah\ nilai\ per\ area\ keamanan\ informasi}{Jumlah\ area\ penilaian}$ x 100%

Keterangan	:	▪ Yang dimaksud dengan Tingkat Keamanan Informasi Pemerintah dilihat dari Indeks KAMI.
		▪ Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi
		▪ Indeks KAMI menilai 5 area pengamanan informasi yaitu
		  ▪ Tata kelola keamanan informasi
		  ▪ Pengelolaan resiko keamanan informasi
		  ▪ Kerangka kerja keamanan informasi
		  ▪ Pengelolaan aset informasi
		  ▪ Teknologi dan keamanan informasi
		▪ Indeks KAMI dilakukan oleh Pemerintah Provinsi, Kabupaten dan Kota secara self assessment untuk kemudian diverifikasi oleh BSSN
		▪ Hasil verifikasi dapat berupa laporan hasil verifikasi BSSN atau sertifikat indeks KAMI yang berlaku satu tahun
		▪ Daerah yang belum pernah melaksanakan atau menyusun Indeks KAMI dapat menyertakan surat keterangan bahwa belum melaksanakan verifikasi

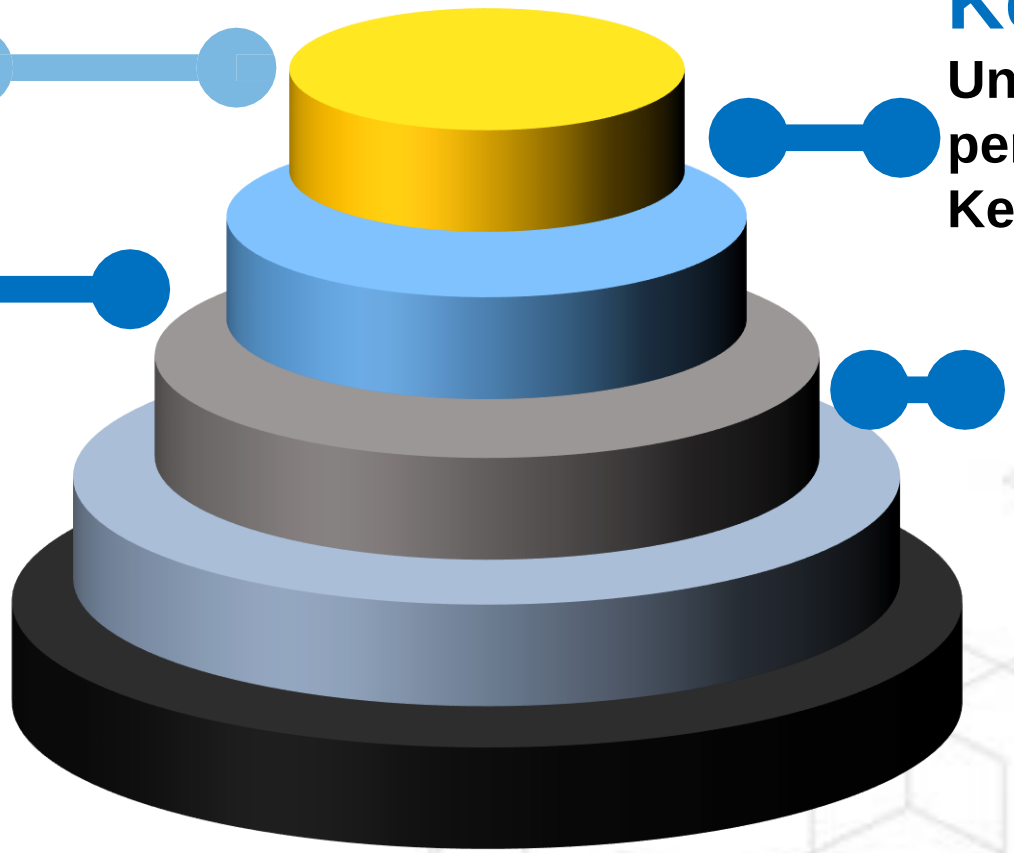
Kunci Keberhasilan Keamanan Informasi

Menerapkan:

SNI ISO/IEC 27001

Tata Kelola Keamanan Informasi:

Komitmen dan Kepedulian Pimpinan untuk mengamankan pengelolaan kebijakan keamanan melalui kepastian prosedur kerja



Manajemen Insiden Keamanan Informasi:

Untuk mengendalikan pengelolaan gangguan Keamanan Informasi

Audit Teknologi Informasi dan Komunikasi

Pemeriksaan paling sedikit 1 kali dalam 1 tahun thd Aset Informasi dan pengujian keamanan sistem

KUNCI UTAMA PADA ORANG DAN BUDAYA

PEOPLE & CULTURE

70%

PROCESS

20%

TOOLS

10%

Ketiga hal tersebut penting dan saling berkaitan

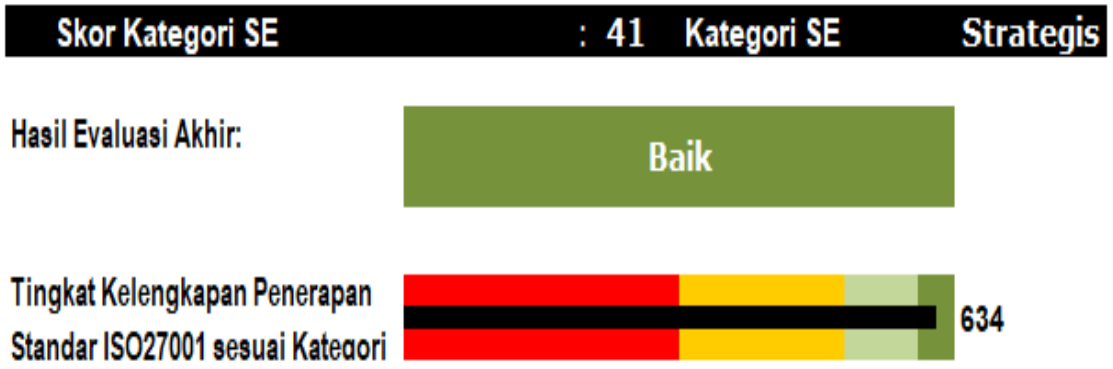
Sumber: Linda Holbeche, Designing more agile structures and ways of working, 2017

TINGKAT KEMATANGAN PEMPROV JATENG

CSM 2022

LEVEL MATURITAS	3,60
Tata Kelola	3,68
Identifikasi	3,49
Proteksi	3,41
Deteksi	3,49
Respon	3,94

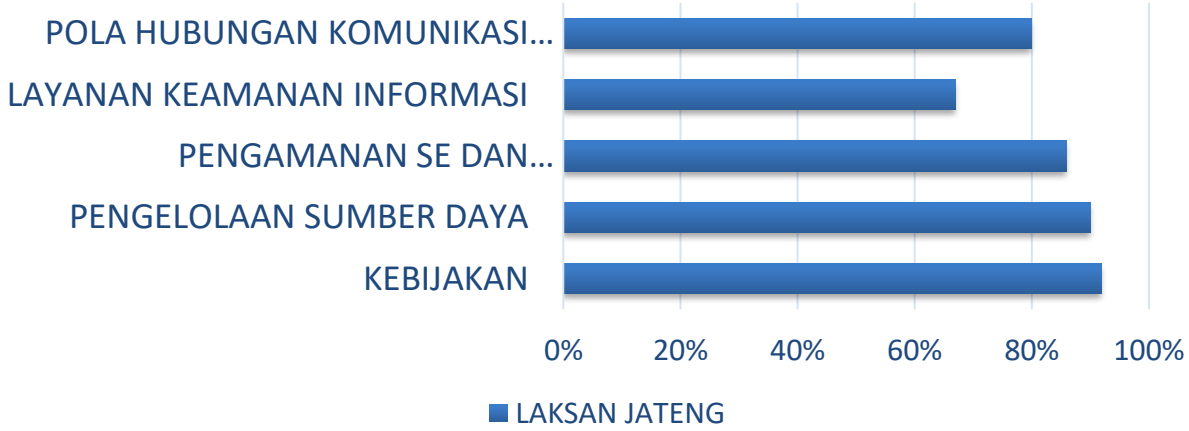
IKAMI 2022



EVA GAR LAKSAN 2022

SKOR
79,079
Status Tingkat Kepatuhan
Cukup

LAKSAN JATENG-2022



SMKI

SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH PROVINSI JATENG

SNI ISO/IEC 27001

Standar Nasional Indonesia International Organization For Standardization/International Electrotechnical Commission 27001

SOP TERKAIT SMKI

..... ?

..... ?

TANGGUNGJAWAB

Melindungi, menjamin kerahasiaan, keutuhan, dan ketersediaan Aset Informasi dalam bentuk data, dokumen, perangkat lunak, aset berwujud dan aset tidak berwujud

Keamanan Informasi Di Pemerintah Daerah

01 Pengguna wajib menggunakan jaringan yang aman.

02 Setiap harddisk/ flashdisk/ media backup lainnya wajib diberi password

03 Perlunya Audit Teknologi Informasi dan Komunikasi (Audit TIK) oleh Tim Internal atau bekerjasama dengan Instansi lain.

04 Pengelolaan data menjadi tanggung jawab Dinas Kominfo, tidak diberikan kepada Dinas lain

05 User & Password akses tidak boleh dipindah tangankan atau diketahui pihak lain

06 Kendali dan pengawasan yang ketat oleh Kepala Dinas, Kabid, Kasi dan jajaran lingkup Diskominfo

07 Saat *idle*/meninggalkan perangkat, aplikasi pastikan sudah kondisi logout.

“(Ingatlah) Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara”

Mayjen TNI Dr. Roebiono Kertopati
(1914 - 1984)
Bapak Persandian Republik Indonesia