



# KEAMANAN DATA DOKUMEN HUKUM DALAM PENGELOLAAN JDIH

**Yon Handri**

**Koordinator Manajemen Risiko dan Pengukuran Tingkat Kematangan Keamanan Siber Pemerintah Pusat, Pertahanan dan Penegakan Hukum  
Direktorat Keamanan Siber dan Sandi Pemerintah Pusat, Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia**

**Badan Siber dan Sandi Negara  
2022**



# KEDAULATAN DATA DI DUNIA SIBER

“Melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial”  
(Pembukaan UUD 1945)

## Amanat Presiden Republik Indonesia

“Kita harus siaga menghadapi ancaman **kejahatan siber**, termasuk **kejahatan penyalahgunaan data**. **Data** adalah jenis kekayaan baru bangsa kita, kini **data** lebih berharga dari minyak. Dalam bidang pertahanan keamanan, kita juga harus tanggap dan siap menghadapi **perang siber**”





# ASPEK REGULASI

UU Pelindungan Data Pribadi Tahun 2022



**UU No.19 Tahun 2016**  
tentang  
Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Pasal 15 ayat (1) setiap PSE harus menyelenggarakan SE secara andal dan aman serta bertanggung jawab terhadap operasinya SE sebagaimana mestinya



**PP 71 Tahun 2019**  
tentang  
Penyelenggaraan Sistem dan Transaksi Elektronik, pada pasal 4, 6, 12 dan 13 terdapat ketentuan yang harus dipenuhi sebagai PSE



**Perpres No. 95 Tahun 2018**  
Tentang SPBE,  
Manajemen keamanan informasi bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi.  
(Pasal 48 ayat (1))



**Peraturan BSSN No.8 Tahun 2020**  
tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik



**Peraturan BSSN No.4 Tahun 2021**  
Tentang Pedoman Manajemen Keamanan SPBE dan Standar Teknis dan Prosedur Keamanan SPBE

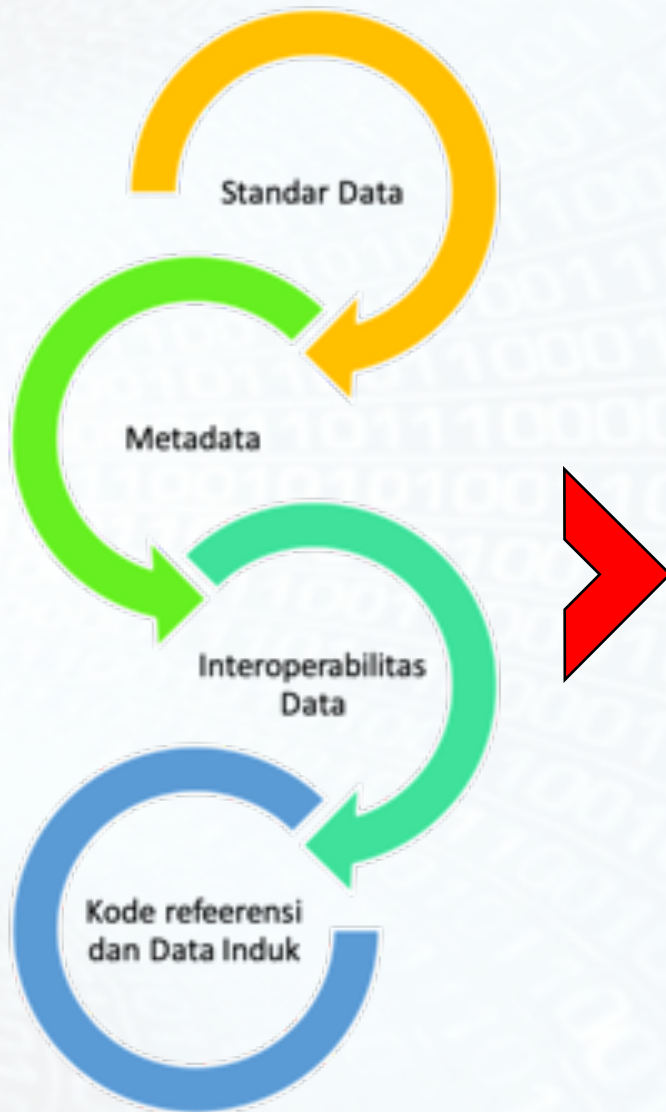
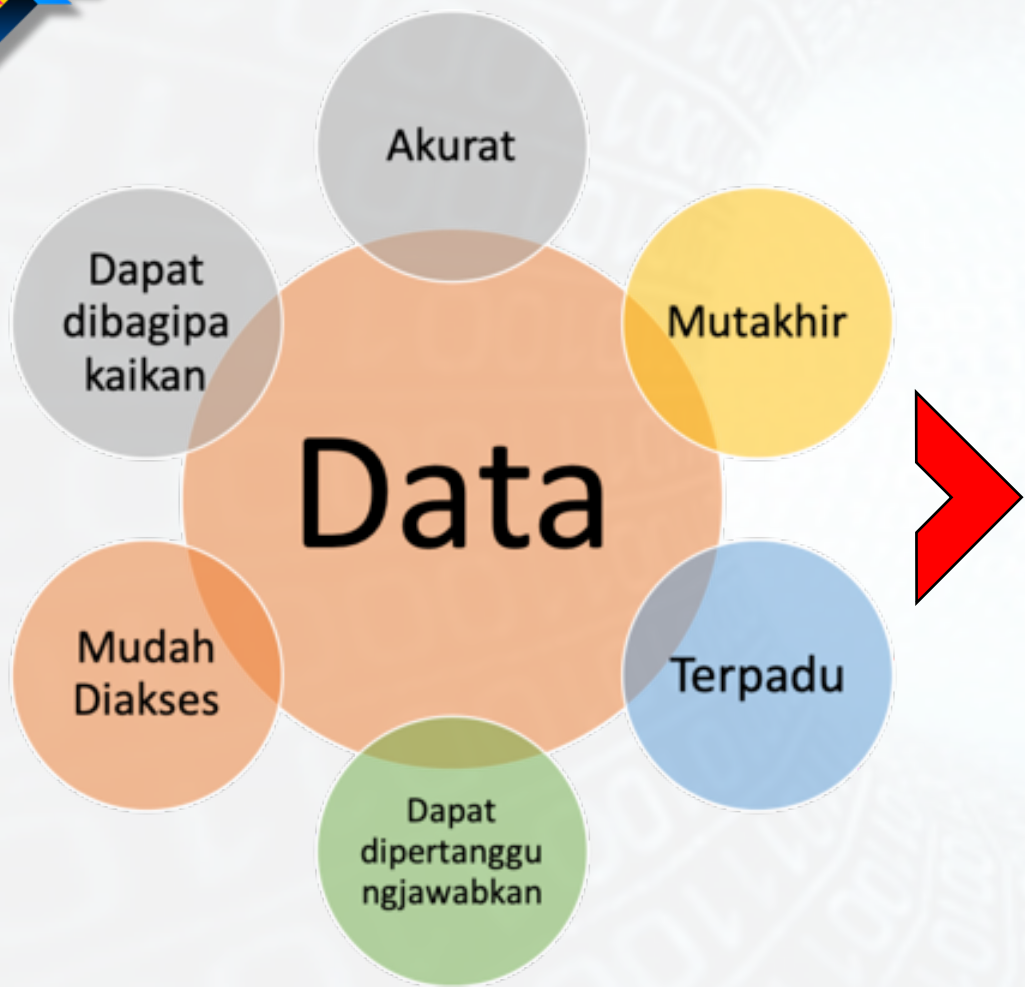
**Perpres No.82 Tahun 2022**  
Tentang Pelindungan Infrastruktur Informasi Vital





# KUALITAS, PRINSIP DAN PELINDUNGAN DATA

PERPRES SDI



UU PDP



## Privasi Data (Data Privacy)

Kepatuhan penggunaan data terhadap hukum dan regulasi perlindungan data dari dikumpulkan, diproses, dibagi, diarsipkan dan dihapus.

UU ITE

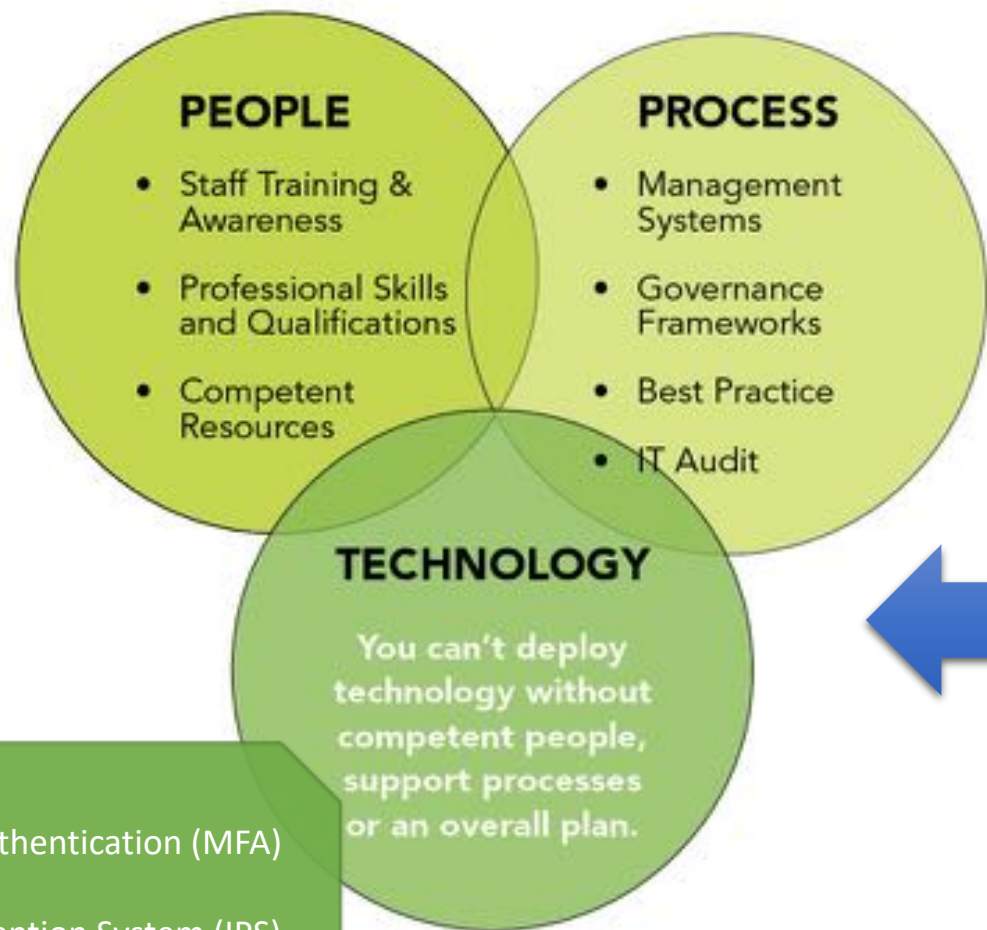


## Keamanan Data (Data Security)

Perlindungan data dari akses ilegal termasuk pada aspek kerahasiaan, keutuhan, ketersediaan dan keaslian data serta kenirsangkalan



# KONSEP DASAR KEAMANAN DATA



- Anti Virus
- Multi Factor Authentication (MFA)
- Firewall
- Intrusion Prevention System (IPS)
- Intrusion Detection System (IDS)
- Virtual Private Network (VPN)
- dll





# CONFIDENTIALITY

## DATA PRIBADI UMUM

- a. nama lengkap;
- b. jenis kelamin;
- c. kewarganegaraan;
- d. agama; dan/atau
- e. Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

## KLASIFIKASI INFORMASI

SANGAT RAHASIA
RAHASIA
TERBATAS
PUBLIK

## DATA PRIBADI SPESIFIK

- a. data dan informasi kesehatan;
- b. data biometrik;
- c. data genetika;
- d. kehidupan/orientasi seksual;
- e. pandangan politik;
- f. catatan kejahatan;
- g. data anak;
- h. data keuangan pribadi; dan/atau
- i. data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

PHONE	: +6281 [REDACTED]
EMAIL	: [REDACTED].id
NAME	: [REDACTED]
GENDER	: Laki-Laki
NIK	: 3174 [REDACTED]
KK	: 3174 [REDACTED]
ADDRESS	: [REDACTED] JAKARTA SELATAN, DKI JAKARTA
DOB	: [REDACTED]
OCCUPATION	: MIRASNASTA
EDUCATION	: DIPLOMA IV/STRATA I
RELIGION	: ISLAM
BLOOD Type	: -
MARRIED STATUS	: KAWIN
FAMILY STATUS	: KEPALA KELUARGA
MOI	: [REDACTED]
DAD	: [REDACTED]
VACCINE ID	: [REDACTED]

**KEBOCORAN DATA**









# INTEGRITY

Rancangan UU PDP Final (Setneg 061219).pdf

Home Tools Rancangan UU P... x

21 / 39 73,6%

Share

BAB XIII  
KETENTUAN PIDANA

Pasal 61

- (1) Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (2) dipidana dengan pidana penjara paling lama 2 (dua) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah).
- (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (3) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp70.000.000.000,00 (tujuh puluh miliar rupiah).

Pasal 62

Setiap Orang yang dengan sengaja dan melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam atau melanggar perlindungan Data Pribadi sebagaimana dimaksud dalam Pasal 52, dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).



Rancangan UU PDP Final (Setneg 061219).pdf

Home Tools Rancangan UU P... x

21 / 39 73,6%

Share

BAB XIII  
KETENTUAN PIDANA

Pasal 61

- (1) Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (2) dipidana dengan pidana penjara paling lama 2 (dua) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah).
- (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (3) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp70.000.000.000,00 (tujuh puluh miliar rupiah).

Pasal 62

Setiap Orang yang dengan sengaja dan melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam atau melanggar perlindungan Data Pribadi sebagaimana dimaksud dalam Pasal 52, dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).





# INTEGRITY

Rancangan UU PDP Final (Setneg 061219).pdf

Home Tools Rancangan UU P... x

21 / 39 73,6%

Signed and all signatures are valid.

KETENTUAN PIDANA

Pasal 61

- (1) Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (2) dipidana dengan pidana penjara paling lama 2 (dua) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah).
- (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (3) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp70.000.000.000,00 (tujuh puluh miliar rupiah).

Pasal 62

Setiap Orang yang dengan sengaja dan melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam atau melanggar perlindungan Data Pribadi sebagaimana dimaksud dalam Pasal 52, dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).



## TANDA TANGAN DIGITAL

Rancangan UU PDP Final (Setneg 061219).pdf

Home Tools Rancangan UU P... x

21 / 39 73,6%

At least one signature is invalid.

KETENTUAN PIDANA

Pasal 61

- (1) Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah).
- (2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (2) dipidana dengan pidana penjara paling lama 2 (dua) tahun atau pidana denda paling banyak Rp20.000.000.000,00 (dua puluh miliar rupiah).
- (3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 51 ayat (3) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak Rp70.000.000.000,00 (tujuh puluh miliar rupiah).

Pasal 62

Setiap Orang yang dengan sengaja dan melawan hukum memasang dan/atau mengoperasikan alat pemroses atau pengolah data visual di tempat umum atau fasilitas pelayanan publik yang dapat mengancam atau melanggar perlindungan Data Pribadi sebagaimana dimaksud dalam Pasal 52, dipidana dengan pidana penjara paling lama 1 (satu) tahun atau pidana denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

# AVAILABILITY

## DATA CENTER TIERS EXPLAINED

Annual global IP traffic will reach **3.3** zettabytes by 2021\*

### 4 TIER FOUR

- Est .04 hours annual downtime
- Usually used by very large companies
- 99.995% availability
- Two independent utility paths
- Fully redundant (2N + 1)
- Can sustain 96-hour power outage

### 3 TIER THREE

- Est 1.6 hours annual downtime
- Usually used by large companies
- 99.982% availability
- Multiple cooling and power paths
- Fault tolerant (N + 1)
- Can sustain 72-hour power outage

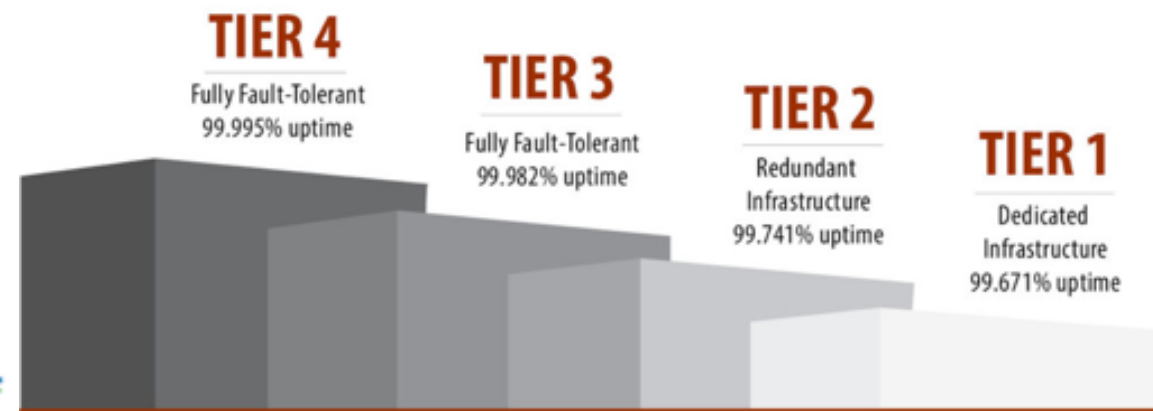
### 2 TIER TWO

- Est 22 hours annual downtime
- Usually used by mid-sized businesses
- 99.749% availability
- Single cooling and power path
- Some redundancy in cooling and power systems

### 1 TIER ONE

- Est 28.8 hours annual downtime
- Usually used by small businesses
- 99.671% availability
- Single cooling and power path
- No redundancy

## DATA CENTER TIERS



\* State Of The Data Center 2018, AFCOM



# STANDAR PERLINDUNGAN DATA

## Peraturan BSSN no 4 tahun 2021

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



### Confidentiality Kerahasiaan

- Menerapkan :
- **Klasifikasi Informasi**
  - Enkripsi Data
  - Kontrol Akses



### Authentication Keaslian

- Menyediakan :
- Mekanisme Verifikasi
  - Mekanisme Validasi
  - Hash Function



### Integrity Keutuhan

- Menerapkan :
- Deteksi Modifikasi
  - Tanda tangan elektronik tersertifikasi



### Non-Repudiation Kenirsangkalan

- Menerapkan :
- Tanda tangan elektronik tersertifikasi
  - Penjaminan PSrE melalui Sertifikat Elektronik



### Availability Ketersediaan

- Menerapkan :
- Sistem pencadangan berkala
  - Perencanaan jaminan selalu dapat diakses
  - Sistem pemulihan





# PERATURAN BSSN NO 4 TAHUN 2021

Pedoman Manajemen Keamanan SPBE dan Standar Tehnis dan Prosedur Keamanan SPBE



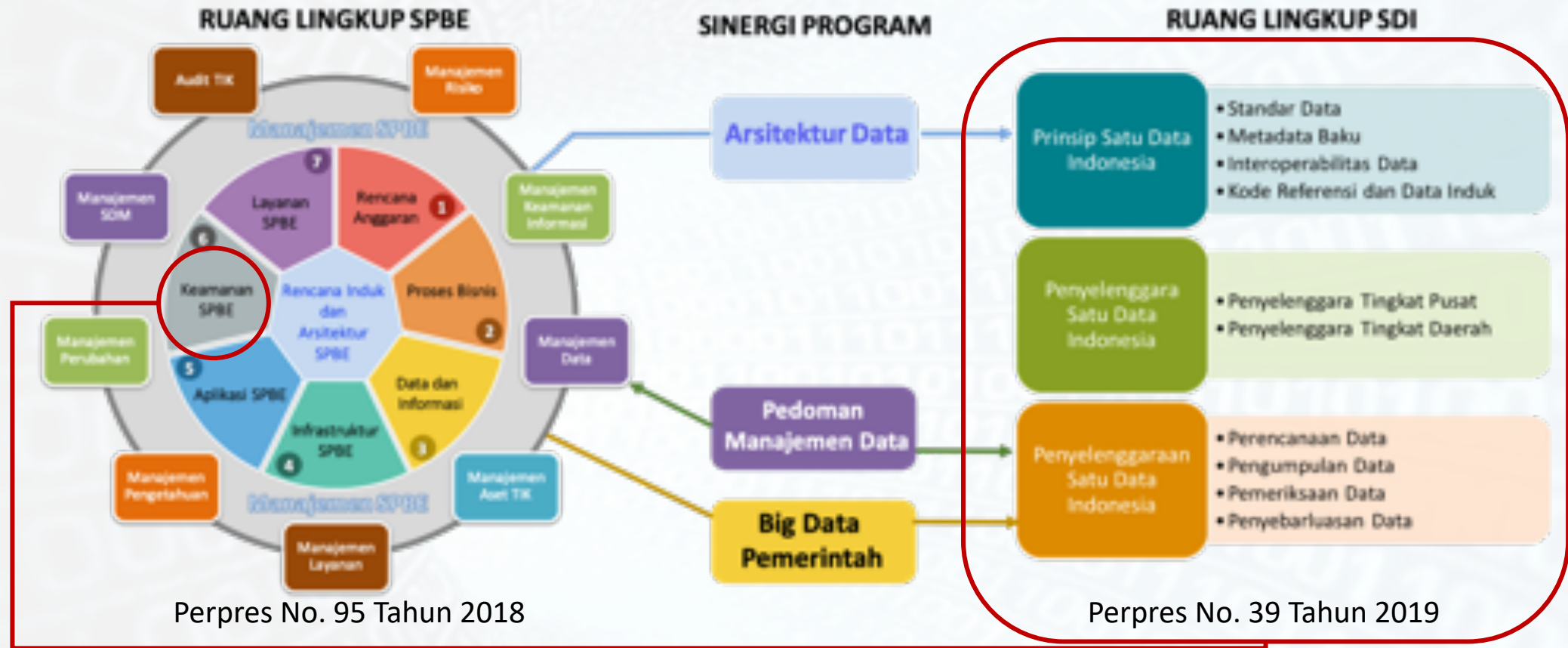
- **Penetapan Ruang Lingkup**
- **Penanggung Jawab**
- **Perencanaan**
- **Dukungan Pengoperasian**
- **Evaluasi Keamanan**
- **Perbaikan berkelanjutan**

## Standar Teknis dan Prosedur Keamanan

01	02	03	04	05
<b>Data &amp; Info</b>	<b>Aplikasi</b>	<b>PDN</b>	<b>JIP</b>	<b>SPL</b>
<ul style="list-style-type: none"><li>• Penerapan Eknripsi</li><li>• Pemanfaatan Serifikat Elektronik</li><li>• Pemulihan &amp; Pencadangan</li></ul>	<ul style="list-style-type: none"><li>• Aplikasi berbasis Web</li><li>• Aplikasi Berbasis Desktop</li><li>• Aplikasi berbasis Mobile</li></ul>	<p>Mengacu pada SNI 8799</p>	<ul style="list-style-type: none"><li>• Administrasi Jaringan</li><li>• Kontrol Akses dan Autentikasi</li><li>• Kontrol Keamanan</li></ul>	<ul style="list-style-type: none"><li>• Interoperabilitas</li><li>• Sistem Terintegrasi</li><li>• Perangkat Integrator</li><li>• API &amp; Web Service</li></ul>



# HUBUNGAN SPBE DENGAN SDI



BSSN bertanggung jawab terhadap kebijakan keamanan SPBE namun BSSN tidak terlibat langsung dalam kebijakan SDI. Meski demikian BSSN tetap memiliki peran penting dalam pengamanan data dan Informasi yang dikelola dalam SDI

“SPBE yang berkualitas mendukung Data yang berkualitas”



# PERATURAN BSSN NO 8 TAHUN 2020

## Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik

### ❖ Model PDCA dalam SNI ISO/IEC 27001:2013



SISTEM MANAJEMEN KEAMANAN INFORMASI		
Konteks Organisasi		
Komitmen Manajemen		
Ruang Lingkup		
Data & Informasi	Aset Pengolah & Penyimpanan Data	Sumber Daya Manusia
Kebijakan Umum	Manajemen Risiko TI	Organisasi SMKI
Keamanan SDM	Pengelolaan Aset	Pengendalian Akses
Manajemen Kriptografi	Keamanan Fisik dan Lingkungan	Keamanan Operasional Sistem Informasi
Keamanan Komunikasi	Akuisisi Pengembangan dan Pemeliharaan Sistem	Hubungan Kerja Dengan Supplier
Kelangsungan Usaha	Penanganan Insiden	Kepatuhan
Identifikasi dan Deteksi	Proteksi	Penanggulangan dan Pemulihan
Pembangunan dan Pengoperasian Security Operation Center (SOC)		
Evaluasi Kinerja		



Tahapan Penerapan SMKI





# KEWAJIBAN PSE PUBLIK

## Pasal 9

### KATEGORI SISTEM ELEKTRONIK

KATEGORI	DESKRIPSI
STRATEGIS	Sistem Elektronik strategis merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, Pelayanan Publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.
TINGGI	Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu
RENDAH	merupakan Sistem Elektronik lainnya yang tidak termasuk STRATEGIS dan TINGGI

(1)

PSE KATEGORI SE STRATEGIS, **wajib menerapkan:**

- a. SNI ISO/IEC 27001;
- b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN; **dan**
- c. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh Kementerian atau Lembaga.

(2)

PSE KATEGORI SE TINGGI, **wajib menerapkan:**

- a. SNI ISO/IEC 27001 **dan/atau** standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN; **dan**
- b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh Kementerian atau Lembaga.

(3)

PSE KATEGORI SE RENDAH, **wajib menerapkan:**

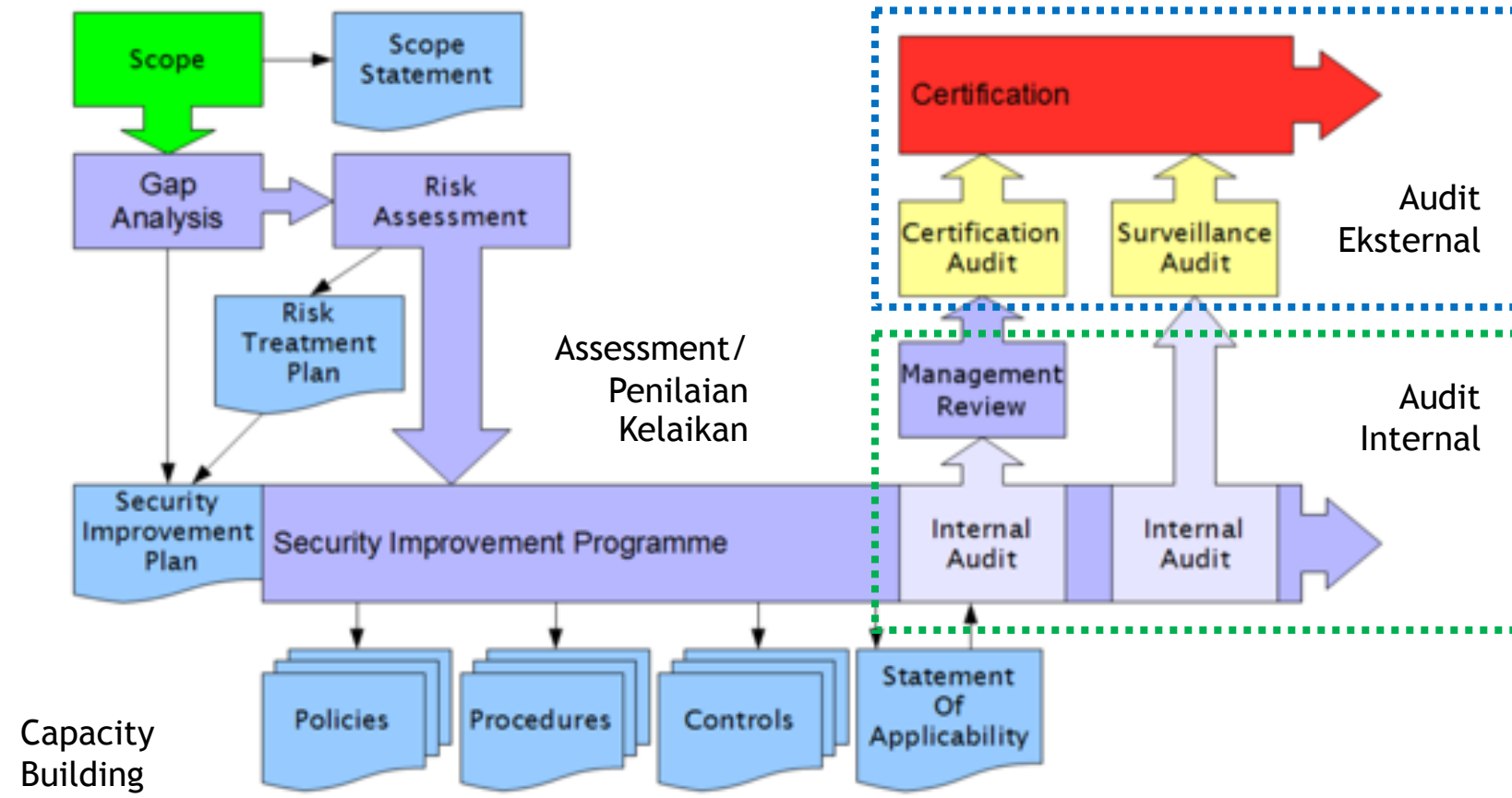
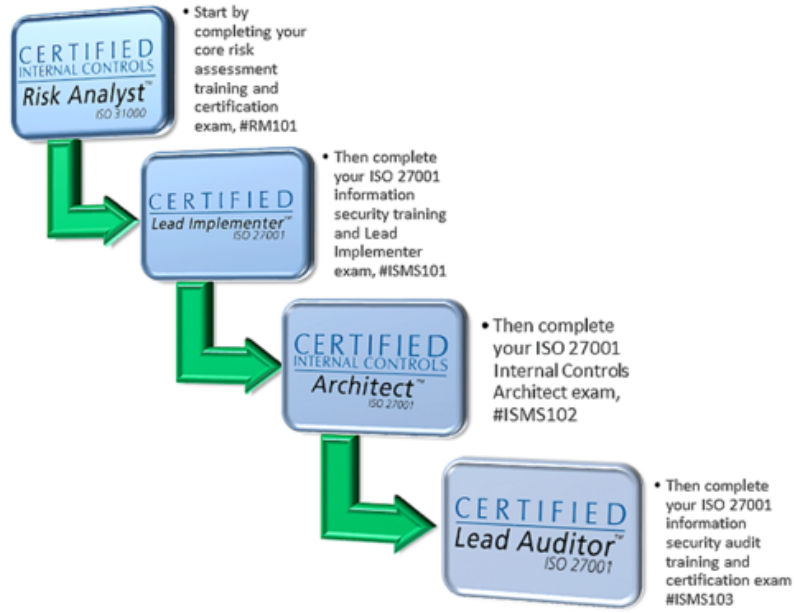
- a. SNI ISO/IEC 27001; **atau**
- b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN

## Pasal 12

“Untuk mempersiapkan penerapan SNI ISO/IEC 27001 sebagaimana dimaksud dalam **Pasal 9**, Penyelenggara Sistem Elektronik **dapat** melakukan penilaian berdasarkan **Indeks KAMI**”



# AUDIT KEAMANAN INFORMASI





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



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