BADAN SIBER DAN SANDI NEGARA

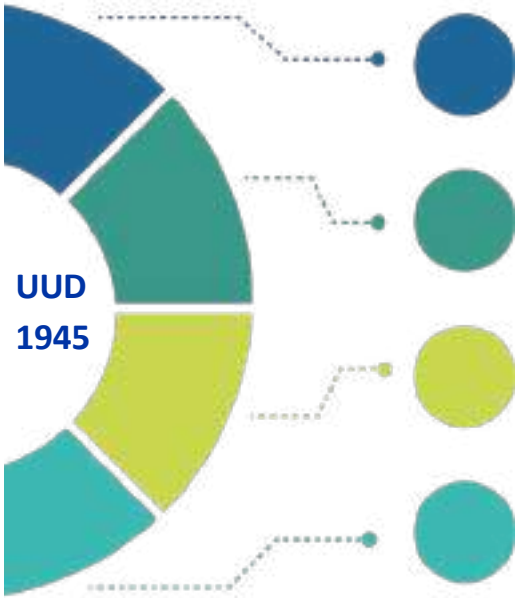
KEAMANAN PEMERINTAH DIGITAL

Direktorat Keamanan Siber dan Sandi Pemerintah Pusat

PROFESIONAL | ELABORATIF | RESPONSIF | INTEGRATIF | SOLID | AKUNTABEL | INOVATIF

DASAR HUKUM KEAMANAN SIBER DI INDONESIA

BADAN SIBER DAN SANDI NEGARA



- UU No. 11/2008 tentang ITE
- UU No. 19/2016 dan UU No. 1/2024 Perubahan UU No.11/2008 tentang ITE
- UU No. 27/2022 tentang Pelindungan Data Pribadi
- UU No. 23/2014 tentang Pemerintah Daerah

PP No.71/2019 ttg Penyelenggaraan Sistem dan Transaksi Elektronik

- Perpres No. 53/2017 tentang BSSN Perpres No. 95/2018 tentang SPBE
- Perpres No. 28/2021 tentang BSSN
- Perpres No. 132/2022 tentang Arsitektur SPBE Nasional
- **Perpres No. 82/2022 tentang Pelindungan IIV**
- Perpres No. 47/2023 Strategi Keamanan Siber Nasional & MKS

- Peraturan BSSN No. 4/2021 tentang Pedoman MKI SPBE dan Standar Teknis
- Peraturan BSSN No. 2/2024 tentang Manajemen Krisis Siber
- Peraturan BSSN No. 5/2024 tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028
- Peraturan BSSN No. 7/2024 tentang Penilaian Kesesuaian Kriteria Umum untuk Evaluasi Keamanan Teknologi Informasi Indonesia
- Peraturan BSSN No. 8/2024 tentang Standar dan Tata Cara Audit Keamanan SPBE
- Peraturan BSSN No. 11/2024 tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi

- Peraturan BSSN No. 7/2023 tentang Identifikasi IIV
- Peraturan BSSN No. 8/2023 tentang Kerangka Kerja Pelindungan IIV
- Peraturan BSSN No. 9/2023 tentang Peningkatan Kapasitas SDM KSS
- Peraturan BSSN No. 10/2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber
- Peraturan BSSN No. 1/2024 tentang Pengelolaan Insiden Siber
- Peraturan BSSN No. 5/2025 tentang Peta Jalan PIIV Sektor Adm. Pemerintahan Tahun 2025 - 2029

PRINSIP KEAMANAN PEMERINTAHAN DIGITAL

Confidentiality

Kerahasiaan: Mencegah akses tidak sah terhadap data/informasi dalam Sistem Pemerintahan Digital.

Authentication

Otentikasi: Memastikan bahwa hanya entitas (user atau sistem) yang sudah ter-otentikasi yang boleh mengakses Sistem Pemerintahan Digital.

Availability

Ketersediaan: Memastikan bahwa sistem dan data selalu tersedia dan dapat diakses saat dibutuhkan oleh pengguna yang sah.

Accounting

Pencatatan: Sistem Pemerintahan Digital harus selalu mencatat seluruh aktivitas untuk keperluan audit, pemantauan, dan pelaporan.

Integrity

Keutuhan: Menjamin bahwa data/informasi tidak diubah tanpa otorisasi

Authorization

Otorisasi: Menentukan *privileged access* (hak atau level akses) apa yang dimiliki entitas setelah otentikasi.

Non-repudiation

Kenirsangkalan: Memastikan bahwa suatu aksi atau transaksi tidak bisa disangkal oleh pihak yang melakukannya.

KERANGKA KERJA KEAMANAN PEMERINTAH DIGITAL

- Dalam rangka memastikan pendekatan ***security by design*** **dan terwujudnya jaminan prinsip keamanan Pemerintah Digital** setiap **Instansi Pusat dan Pemerintah Daerah** harus melaksanakan tata kelola dan manajemen Keamanan Pemerintah Digital sesuai dengan ketentuan peraturan perundang-undangan.
- Pelaksanaan tata kelola dan manajemen Keamanan Pemerintah Digital didukung melalui pelaksanaan kerangka kerja Keamanan Pemerintah Digital yaitu Identifikasi, Proteksi, Deteksi, Penanggulangan dan Pemulihan.

BADAN SIBER DAN SANDI NEGARA

State of Data

BADAN SIBER DAN SANDI NEGARA

Kontrol Penggunaan Algoritma Kriptografi

1. Penerapan sistem enkripsi data (in use, in transit dan at rest);
2. Mekanisme verifikasi;
3. Pendeteksian modifikasi;
4. Menerapkan SSL atau TLS versi terbaru untuk proses transmisi data :
   - TLS 1.2 keatas
   - Penggunaan cipher suite yang kuat (AES-GCM)
5. Perlindungan API token (JWT) - RBG, Sign;
6. Penerapan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
7. Kriptografi untuk verifikasi statis.

Peraturan BSSN No 11 Tahun 2024

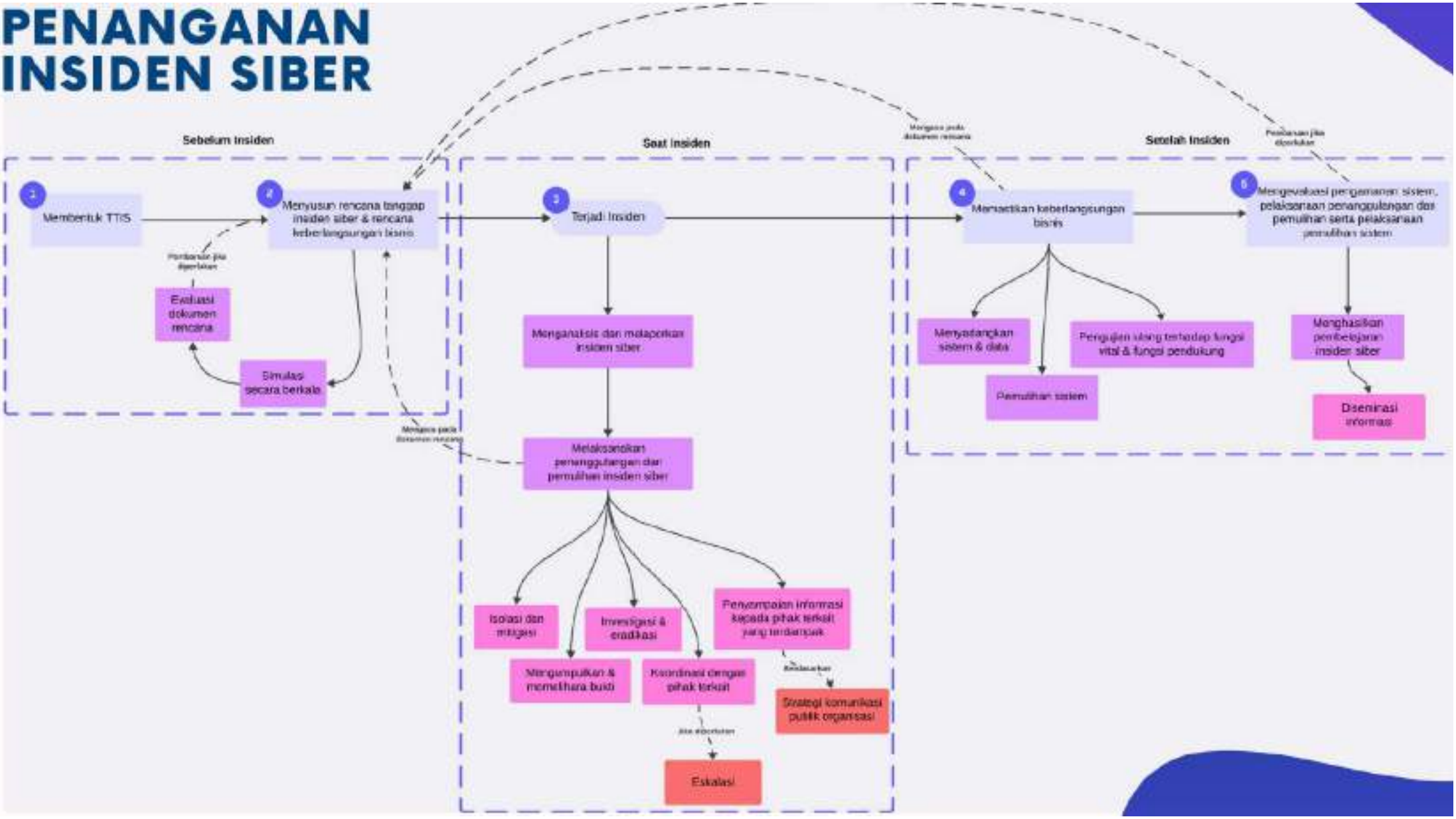
Penyelenggaraan Algoritma Kriptografi Indonesia Dan Penilaian Kesesuaian Keamanan Modul Kriptografi

B. SISTEM ELEKTRONIK TINGGI

c	Jenis Algoritma Kriptografi	Nama Algoritma
1	2	3
1	Sandi Blok (Block Cipher)	AES-192 AES-256 Camellia-192 Camellia-256
2	Sandi Alir (Stream Cipher)	HC-128 Salsa 20/20 Sosemanuk ChaCha20
3	Fungsi Hash (Hash Function)	SHA-384 SHA-512/256 Whirlpool SHA3-256 SHA3-384 SHA3-512 SHAKE256

https://www.bssn.go.id/daftar-algoritma-kriptografi-indonesia/

PENANGANAN INSIDEN SIBER



Indikator 10 TK Keamanan Siber (IKASANDI)

Deskripsi

Kemampuan/kapabilitas dari IPPD dalam menyelenggarakan keamanan Pemerintah Digital meliputi implementasi tata kelola dan manajemen keamanan informasi, serta implementasi kontrol teknis keamanan berdasarkan Instrumen Pengukuran Kematangan Keamanan Siber dan Sandi (IKASANDI).

Dasar Hukum

1. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital
2. Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi IIV
3. Peraturan BSSN Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber

Instansi Pembina

Fungsi Instansi

Fungsi Teknologi, Informasi, dan Komunikasi.

Fungsi Pengelola Layanan Digital

Objek yang diukur

Ikasandi area Keamanan Siber terdiri dari domain :

- Identifikasi
- Proteksi
- Deteksi
- Penanggulangan dan Pemulihan

Indikator 10 TK Keamanan Siber (IKASANDI)

Domain Identifikasi : Memahami Aset dan Risiko

Domain Identifikasi mencakup inventarisasi aset, penilaian risiko, dan analisis ancaman. Merupakan tahap awal fundamental untuk mengetahui apa yang perlu dilindungi.

Tanpa pemahaman kuat tentang aset dan risiko, langkah proteksi dan deteksi tidak efektif. Domain ini menjadi fondasi perencanaan strategis keamanan siber.

Fungsi Domain

- Inventarisasi dan klasifikasi aset
- Penilaian risiko keamanan informasi
- Analisis ancaman dan kerentanan
- Manajemen risiko rantai pasok

Lima Sub-Kategori Kontrol

Kebijakan dan Organisasi Keamanan Informasi

Komitmen pimpinan, kebijakan, struktur tim SMKI

Perencanaan dan Manajemen Aset

Inventarisasi, klasifikasi, dan penanggung jawab aset

Mengelola Aset Informasi

Klasifikasi data, retensi, dan pemusnahan data

Menilai dan Mengelola Risiko

Kerangka risiko, identifikasi, penilaian, dan mitigasi

Mengelola Risiko Rantai Pasok

Vendor, cloud, dan pihak ketiga

Indikator 10 TK Keamanan Siber (IKASANDI)

Domain Proteksi : Lini Pertahanan Keamanan Siber

Domain Proteksi berfokus pada implementasi kontrol untuk melindungi sistem dan data dari ancaman. Merupakan lini pertama pertahanan yang mengurangi kemungkinan terjadinya insiden.

Investasi dalam proteksi yang kuat dapat mengurangi frekuensi dan dampak insiden keamanan secara signifikan.

Fungsi Domain

- Kontrol akses dan manajemen identitas
- Enkripsi dan pengamanan data
- Keamanan infrastruktur dan aplikasi
- Kebijakan keamanan dan kesadaran SDM

Enam Sub-Kategori Kontrol Proteksi

Manajemen Identitas dan Akses

Autentikasi, otorisasi, dan hak akses

Keamanan Sumber Daya Manusia

Kesadaran, pelatihan, dan disiplin keamanan

Manajemen Kelemahan dan Pembaruan

Patch management dan vulnerability handling

Pengamanan Infrastruktur

Jaringan, endpoint, dan perimeter security

Pengamanan Aplikasi dan Data

Secure coding, enkripsi, dan backup

Keamanan Fisik

Lingkungan dan akses fisik

Indikator 10 TK Keamanan Siber (IKASANDI)

Domain Deteksi : Pemantauan dan Analisis Ancaman

Domain Deteksi melibatkan pemantauan kontinu, analisis log, dan penggunaan alat untuk mengidentifikasi aktivitas mencurigakan atau pelanggaran.

Deteksi efektif adalah kunci untuk merespons insiden dengan cepat. Memastikan ancaman dapat dikenali segera setelah muncul sebelum menyebabkan kerusakan signifikan.

Fungsi Domain

- Pemantauan log dan event secara real-time
- Deteksi anomali dan intrusion
- Pengujian keamanan berkala
- Analisis ancaman dan intelijen

Tiga Sub-Kategori Kontrol Deteksi

Pemantauan dan Analisis Log

Monitoring log keamanan, analisis event, dan pelaporan insiden potensial secara berkelanjutan

Deteksi Intrusion dan Anomali

IDS/IPS, behavioral analytics, dan threat detection untuk mengenali aktivitas mencurigakan

Penilaian dan Pengujian Keamanan

Vulnerability assessment, penetration testing, dan security audit secara periodik

Indikator 10 TK Keamanan Siber (IKASANDI)

Domain Gulih : Penanggulangan Pemulihan

Domain ini mencakup tanggapan terhadap insiden yang terdeteksi, mitigasi dampak, isolasi sistem, perbaikan, dan pemulihan operasional.

Bertujuan untuk meminimalkan dampak insiden dan memastikan pemulihan cepat serta efektif. Respon yang baik mengurangi kerugian dan mempercepat pemulihan operasional.

Fungsi Domain

- Persiapan dan perencanaan tanggap insiden
- Deteksi, analisis, dan kontainment insiden
- Eradikasi dan pemulihan sistem
- Pembelajaran dan perbaikan pasca-insiden

Tiga Sub-Kategori Kontrol Penanggulangan dan Pemulihan

Persiapan dan Perencanaan

Tim CSIRT, playbook insiden, komunikasi, dan pelatihan tanggap darurat keamanan siber

Proses Tanggap Insiden

Identifikasi, kontainment, eradikasi, dan pemulihan dengan dokumentasi lengkap

Pemulihan dan Pembelajaran

Business continuity, disaster recovery, dan lessons learned untuk penguatan sistem

Indikator 10 TK Keamanan Siber (IKASANDI)

Kurang/*Initiate* (1 ≤ nilai ≤ 1,5)

Kriteria

1. Dalam tahap penyusunan tata kelola dan manajemen keamanan informasi.
2. Dalam tahap identifikasi Infrastruktur Informasi Vital oleh Instansi Pemerintah.

Kondisi

Pelaksanaan tata kelola dan manajemen keamanan informasi dilaksanakan sesuai dengan kebutuhan instansi dan bersifat terbatas pada layanan digital tertentu.

Data Dukung:

1. Nilai IKASANDI pada area Keamanan Siber.
   0 < IKASANDI < 1,5

Indikator 10 TK Keamanan Siber (IKASANDI)

Cukup/*Emerging* (1,5 < nilai ≤ 2,5)

Kriteria

1. Instansi Pemerintah telah menerapkan tata kelola manajemen keamanan informasi sesuai dengan pedoman.
2. Penerapan tata kelola manajemen keamanan informasi sesuai dengan substansi Rencana Aksi Nasional Pemerintah Digital pada perencanaan Instansi Pemeirntah.
3. Telah melakukan identifikasi Infrastruktur Informasi Vital.

Kondisi

Tersedianya hasil pengukuran kematangan keamanan Pemerintah Digital, dan identifikasi Infrastruktur Informasi Vital oleh Penyelenggara Sistem Elektronik (PSE)/Layanan Digital Pemerintah **Instansi Pemerintah secara mandiri.**

Data Dukung:

1. Dokumentasi Identifikasi Infrastruktur Informasi Vital*.

1. Nilai IKASANDI pada area Keamanan Siber. 1,50 < IKASANDI < 2,50

Indikator 10 TK Keamanan Siber (IKASANDI)

Baik/*Developing* (2,5 < nilai ≤ 3,5)

Kriteria

1. Instansi Pemerintah telah menerapkan tata kelola manajemen keamanan informasi sesuai dengan pedoman.
2. Telah melaksanakan implementasi kontrol teknis berdasarkan hasil kematangan keamanan siber.

Kondisi

Hasil pengukuran Tingkat Kematangan Keamanan Pemerintah Digital **telah diverifikasi** oleh lembaga yang menyelenggarakan tugas pemerintahan di **bidang siber dan sandi dan/atau pemerintah daerah** yang diberikan kewenangan sesuai dengan peraturan perundang-undangan.

Pengukuran Ikasandi Terverifikasi

Data Dukung:

1. Nilai IKASANDI pada area Keamanan Siber.
   2,50 < IKASANDI < 3,50

Indikator 10 TK Keamanan Siber (IKASANDI)

Sangat Baik/*Embedded* (3,5 < nilai ≤ 4)

Kriteria

Tata kelola manajemen keamanan Instansi Pemerintah telah terorganisir, terkelola secara terpadu, dan optimal, serta dilaksanakan reviu secara berkala.

Kondisi

Hasil pengukuran Tingkat Kematangan Keamanan Pemerintah Digital telah diverifikasi oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang siber dan sandi dan/atau pemerintah daerah yang diberikan kewenangan sesuai dengan peraturan perundang-undangan.

Pengukuran Ikasandi Terverifikasi

Data Dukung:

1. Instrumen IKASANDI pada area Keamanan Siber. 3,50 < IKASANDI < 4,00

Indikator 10 TK Keamanan Siber (IKASANDI)

Memuaskan/*Leading* (4 < nilai ≤ 5)

Kriteria

Penerapan tindak lanjut sesuai reviu atas Keamanan Pemerintah Digital Instansi Pemerintah melalui proses otomasi.

Kondisi

Hasil pengukuran Tingkat Kematangan Keamanan Pemerintah Digital telah diverifikasi oleh lembaga yang melaksanakan tugas pemerintahan di bidang keamanan Pemerintah Digital dan sandi dan/atau pemerintah daerah yang diberikan kewenangan sesuai dengan peraturan perundang-undangan.

Rekomendasi hasil penilaian telah ditindaklanjuti melalui perbaikan berkelanjutan.

Perbaikan berkelanjutan Keamanan Pemerintah Digital telah menjadi bagian budaya organisasi.

Pengukuran Ikasandi Terverifikasi

Data Dukung:

1. Instrumen IKASANDI pada area Keamanan Siber 4,00 < IKASANDI < 5,00

Indikator 11 TK Penerapan Kriptografi untuk Keamanan Data (IKASANDI)

Domain Persandian

Mengukur tingkat kepatuhan dan pemenuhan kondisi terhadap pengamanan informasi melalui lima area evaluasi yang mencakup aspek kebijakan, sumber daya, sistem, layanan, dan komunikasi sandi.

Persandian

5.1 Kebijakan Pengamanan Informasi	5.2 Pengelolaan Sumber Daya	5.3 Pengamanan Sistem Elektronik dan Informasi non Elektronik	5.4 Layanan Keamanan Informasi	5.5 Pola Hubungan Komunikasi Sandi
Rencana strategis pengamanan informasi, arsitektur keamanan informasi, dan tata kelola keamanan informasi	Aset TIK, materiil sandi, sumber daya manusia, manajemen pengetahuan, dan pengembangan kompetensi	Pengamanan sistem elektronik dan pengamanan informasi nonelektronik secara komprehensif	Penetapan program kerja layanan keamanan informasi dan evaluasi pelaksanaannya secara berkala	Identifikasi dan analisis pola hubungan komunikasi sandi secara sistematis

Indikator 11 TK Penerapan Kriptografi untuk Keamanan Data (IKASANDI)

Kurang/*Initiate* (1 ≤ nilai ≤ 1,5)

Kriteria

Dalam tahap penyiapan penerapan teknologi kriptografi untuk keamanan data, sesuai dengan peraturan perundang-undangan.

Kondisi

Penerapan teknologi kriptografi dilaksanakan secara sewaktu-waktu atau bersifat terbatas pada layanan digital tertentu.

Data Dukung:

Laporan pelaksanaan penerapan teknologi kriptografi.

Indikator 11 TK Penerapan Kriptografi untuk Keamanan Data (IKASANDI)

Cukup/*Emerging* (1,5 < nilai ≤ 2,5)

Kriteria

Sudah menerapkan teknologi kriptografi sesuai dengan peraturan perundang-undangan pada sebagian Layanan Digital Pemerintah.

Kondisi

1. Teknologi kriptografi diterapkan pada 1 (satu) siklus data (at-rest, in-transit, dan/atau in-use) terhadap **≤ 50%** dari total Layanan Digital Pemerintah dengan minimal kategorisasi Sistem Elektronik (SE)/Layanan Digital Pemerintah pada tingkat tinggi.

2. Algoritma kriptografi yang digunakan sesuai dengan peraturan perundang-undangan pada sebagian Layanan Digital Pemerintah.

Sesuai Keputusan Kepala BSSN Nomor 443 Tahun 2025 tentang Algoritma Kriptografi Indonesia

Data Dukung:

Laporan pelaksanaan penerapan teknologi kriptografi.

Indikator 11 TK Penerapan Kriptografi untuk Keamanan Data (IKASANDI)

Baik/*Developing* (2,5 < nilai ≤ 3,5)

Kriteria

Teknologi kriptografi telah diterapkan pada sebagian Layanan Digital Pemerintah di 2 (dua) siklus data.

Kondisi

1. Teknologi kriptografi diterapkan minimal di 2 (dua) siklus data (at-rest dan in- transit; atau at-rest dan in-use; atau in-transit dan in-use) terhadap **≤ 50%** dari total Layanan Digital Pemerintah dengan minimal kategorisasi Sistem Elektronik (SE)/Layanan Digital Pemerintah pada tingkat tinggi.

Data Dukung:

Laporan pelaksanaan penerapan teknologi kriptografi.

Indikator 11 TK Penerapan Kriptografi untuk Keamanan Data (IKASANDI)

Sangat Baik/*Embedded* (3,5 < nilai ≤ 4)

Kriteria

1. Teknologi kriptografi telah diterapkan pada seluruh Layanan Digital Pemerintah prioritas dan/atau Layanan Digital Pemerintah tematik di 2 (dua) siklus data.
2. Telah dilakukan evaluasi pada penerapan teknologi kriptografi.

Kondisi

1. Teknologi kriptografi diterapkan minimal di 2 (dua) siklus data (at-rest dan in-transit; atau at-rest dan in-use; atau in-transit dan in-use) pada 100% Sistem Elektronik dengan minimal kategorisasi Sistem Elektronik (SE)/Layanan Digital Pemerintah pada tingkat tinggi.

1. Evaluasi penerapan teknologi kriptografi telah dilakukan pada seluruh Layanan Digital Pemerintah prioritas dan/atau Layanan Digital Pemerintah tematik

Data Dukung:

Laporan evaluasi penerapan teknologi kriptografi.

Indikator 11 TK Penerapan Kriptografi untuk Keamanan Data (IKASANDI)

Memuaskan/*Leading* (4 < nilai ≤ 5)

Kriteria

1. Telah melakukan tindak lanjut hasil evaluasi pada penerapan teknologi kriptografi.

Kondisi

1. Optimalisasi penerapan teknologi kriptografi telah dilaksanakan secara menyeluruh.
2. Penerapan teknologi kriptografi telah menjadi budaya kerja untuk mendukung kualitas Layanan Digital Pemerintah.
3. Penyelenggaraan persandian telah terorganisir dan terkelola dengan baik

Data Dukung:

1. Laporan tindak lanjut hasil evaluasi penerapan teknologi kriptografi.
2. Nilai IKASANDI pada Area Kematangan Persandian 4,00 < IKASANDI < 5,00

Pengukuran Ikasandi Terverifikasi

Indikator 12 TK Kapabilitas Penanganan Insiden Siber (IKASANDI)

Deskripsi

Kemampuan/kapabilitas dari Instansi Pemerintah dalam Penanganan Insiden Siber secara komprehensif, terstruktur, dan terstandar berdasarkan IKASANDI pada Area Penanganan Insiden Siber, termasuk di dalamnya memanfaatkan Tim Tanggap Insiden Siber (TTIS) atau *Computer Security Incident Response Team* (CSIRT) di Instansi masing-masing hingga kolaborasi dengan TTIS Nasional.

Dasar Hukum

1. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital
2. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber
3. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber

Instansi Pembina

- Fungsi Organisasi dan Tata Laksana.
- Fungsi SDM.
- Fungsi Teknologi, Informasi, dan Komunikasi.
- Fungsi Pengelola Layanan Digital.

Objek yang diukur

IKASANDI pada area Penanganan Insiden Siber

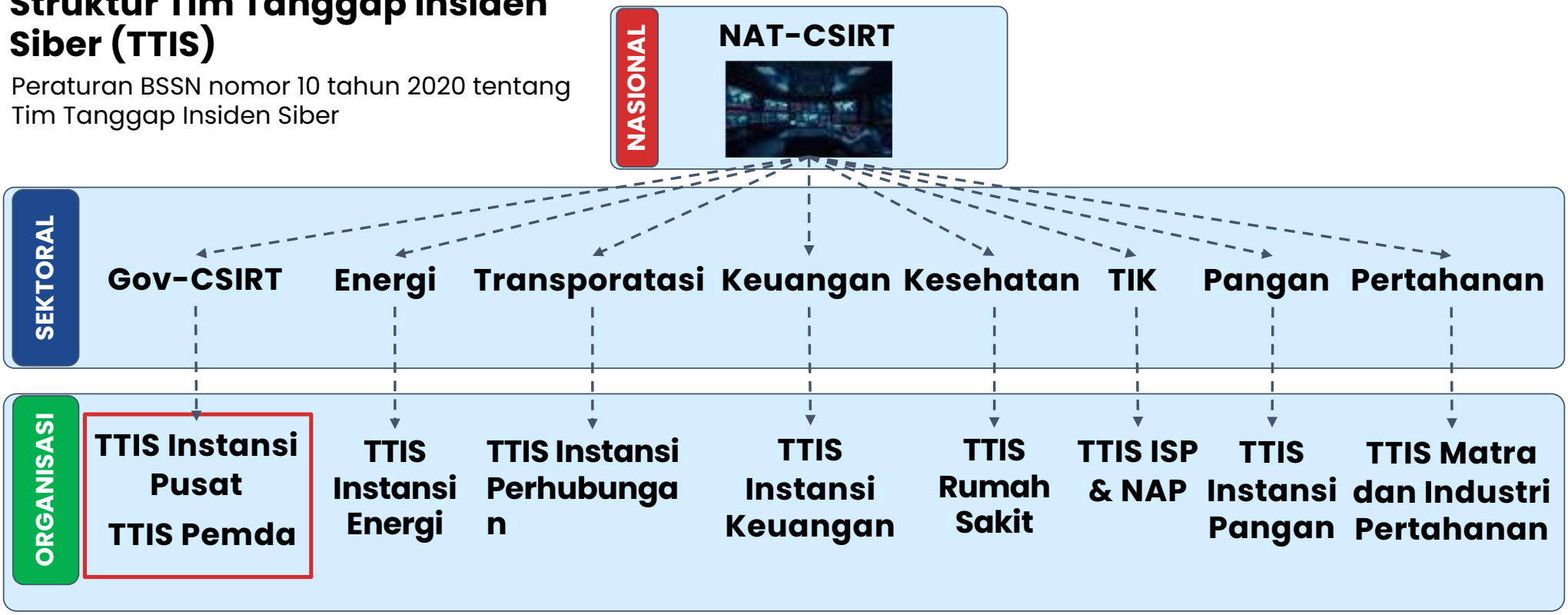
Instansi Pembina

Indikator 12 TK Kapabilitas Penanganan Insiden Siber (IKASANDI)

Tim Tanggap Insiden Siber

Struktur Tim Tanggap Insiden Siber (TTIS)

Peraturan BSSN nomor 10 tahun 2020 tentang Tim Tanggap Insiden Siber



Indikator 12 TK Kapabilitas Penanganan Insiden Siber (IKASANDI)

Tim Tanggap Insiden Siber

Tahapan Registrasi

Asistensi TTIS

1. Memahami regulasi TTIS
2. Memahami tujuan TTIS
3. Memahami model dan mekanisme kerja TTIS
4. Memahami SDM TTIS
5. Memahami Layanan-Layanan TTIS
6. Memahami Pendanaan TTIS

Perencanaan TTIS

1. Perumusan visi dan misi TTIS
2. Perumusan Struktur Organisasi TTIS
3. Identifikasi Layanan TTIS
4. Identifikasi Kebutuhan SDM TTIS
5. Identifikasi Kebutuhan Perangkat/tools TTIS
6. Penyusunan Kebijakan dan SOP
7. Penyusunan Rencana Kerja & anggaran

Penerapan TTIS

1. Pengangkatan Tim TTIS
2. Pemenuhan Perangkat/Tools TTIS
3. Penerapan Kebijakan dan SOP
4. Deklarasi TTIS (Menggunakan RFC 2350)
5. Registrasi TTIS (Mengirim Berkas registrasi TTIS ke BSSN melalui email)
6. Launching TTIS

TTIS Terbentuk

- SK tentang TTIS
- Surat Kesediaan Menjadi Narahubung TTIS

TTIS Teregistrasi

- Surat Permohonan Pendaftaran TTIS
- Formulir Registrasi TTIS
- RFC 2350
- Dokumen Sumber Daya Penyelenggara TTIS

Indikator 12 TK Kapabilitas Penanganan Insiden Siber (IKASANDI)

Kurang/*Initiate* (1 ≤ nilai ≤ 1,5)

Kriteria

1. Dalam tahap penyiapan untuk Penanganan Insiden Siber pada Layanan Digital Pemerintah.
2. Penanganan Insiden Siber pada Layanan Digital Pemerintah dilaksanakan sesuai kebutuhan Instansi Pemerintah.

Kondisi

1. Penanganan Insiden Siber dilaksanakan secara sewaktu-waktu atau bersifat terbatas pada layanan digital tertentu,

1. Dalam Tahap Penyiapan TTIS.

Data Dukung:

1. Dokumentasi pelaksanaan penanganan insiden.
2. Nilai IKASANDI pada area Penanganan Insiden Siber.
   0 < IKASANDI < 1,50

Indikator 12 TK Kapabilitas Penanganan Insiden Siber (IKASANDI)

Cukup/*Emerging* (1,5 < nilai ≤ 2,5)

Kriteria

1. IPPD telah membentuk TTIS sesuai dengan pedoman dan perencanaan yang terarah.
2. Penanganan insiden siber telah dilakukan oleh TTIS pada sebagian Layanan Digital Pemerintah.

Kondisi

1. Instrumen IKASANDI area Penanganan Insiden Siber (Self-Assessment)

1. Tersedianya hasil pengukuran kematangan keamanan siber area Penanganan Insiden Siber secara mandiri.

1. IPPD memiliki TTIS yang teregistrasi di TTIS Nasional.

Data Dukung:

1. Penetapan TTIS.

1. Nilai IKASANDI pada area Penanganan Insiden Siber. 1,50 < IKASANDI < 2,50

Indikator 12 TK Kapabilitas Penanganan Insiden Siber (IKASANDI)

Baik/*Developing* (2,5 < nilai ≤ 3,5)

Kriteria

1. Instansi Pemerintah telah melaksanakan Penanganan Insiden Siber melalui TTIS.
2. Penanganan insiden siber telah dilakukan oleh TTIS pada seluruh Layanan Digital Pemerintah prioritas dan/atau Layanan Digital Pemerintah tematik.

Kondisi

1. Pelaksanaan Penanganan Insiden Siber telah dilaksanakan secara terstandar dan terstruktur dalam TTIS sesuai dengan Substansi **Rencana Aksi Nasional Pemerintah Digital** pada perencanaan Instansi Pemerintah.

1. Hasil pengukuran tingkat kematangan keamanan siber area Penanganan Insiden Siber telah diverifikasi oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang siber dan sandi dan/atau pemerintah daerah yang diberikan kewenangan sesuai dengan peraturan perundang-undangan.

1. TTIS IPPD telah berkolaborasi dengan TTIS Nasional.

Pengukuran Ikasandi Terverifikasi

Indikator 12 TK Kapabilitas Penanganan Insiden Siber (IKASANDI)

Sangat Baik/*Embedded* (3,5 < nilai ≤ 4)

Kriteria

1. Kapabilitas Penanganan Insiden Siber melalui TTIS Instansi Pemerintah telah direviu secara berkala.
2. TTIS berpartisipasi aktif untuk berbagi informasi dan/atau sumber daya dengan TTIS lainnya dalam lingkup nasional.

Kondisi

Hasil pengukuran tingkat kematangan keamanan siber area Penanganan Insiden Siber telah diverifikasi oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang siber dan sandi dan/atau pemerintah daerah yang diberikan kewenangan sesuai dengan peraturan perundang-undangan.

Pengukuran Ikasandi Terverifikasi

Data Dukung:

Instrumen IKASANDI area Penanganan Insiden Siber.
3,50 < IKASANDI < 4,00

Indikator 12 TK Kapabilitas Penanganan Insiden Siber (IKASANDI)

Memuaskan/*Leading* (4 < nilai ≤ 5)

Kriteria

1. Pelaksanaan penanganan insiden oleh TTIS Instansi Pemerintah telah dievaluasi untuk perbaikan berkelanjutan.
2. Optimalisasi penanganan insiden siber Instansi Pemerintah memberikan dampak terhadap kapabilitas keamanan Pemerintah Digital nasional.

Kondisi

1. Hasil pengukuran tingkat kematangan keamanan siber area Penanganan Insiden Siber **telah diverifikasi** oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang siber dan sandi dan/atau pemerintah daerah yang diberikan kewenangan sesuai dengan peraturan perundang-undangan.

1. Rekomendasi hasil penilaian telah ditindaklanjuti melalui perbaikan berkelanjutan.

Data Dukung:

1. Instrumen IKASANDI area Penanganan Insiden Siber 4,00 < IKASANDI < 5,00

Pengukuran Ikasandi Terverifikasi

PENJELASAN INDIKATOR
KEAMANAN PEMERINTAH DIGITAL

Profesional | Elaboratif | Responsif | Integratif | Solid | Akuntabel | Inovatif

PERSYARATAN INDIKATOR 10

BADAN SIBER DAN SANDI NEGARA

INDIKATOR 10

Tingkat Kematangan Keamanan Pemerintah Digital

NILAI IKASANDI PADA AREA KEAMANAN SIBER

Hasil *self assessment*/verifikasi

- **Level 1:** Nilai IKASANDI pada area Keamanan Siber 0 ≤ IKASANDI < 1,50
- **Level 2:** Nilai IKASANDI pada area Keamanan Siber 1,50 ≤ IKASANDI < 2,50

Hasil verifikasi

- **Level 3:** Nilai IKASANDI pada area Keamanan Siber 2,50 ≤ IKASANDI < 3,50
- **Level 4:** Nilai IKASANDI pada area Keamanan Siber 3,50 ≤ IKASANDI < 4,00
- **Level 5:** Nilai IKASANDI pada area Keamanan Siber 4,00 ≤ IKASANDI ≤ 5,00

IDENTIFIKASI INFRASTRUKTUR INFORMASI VITAL

Data Dukung untuk **Level 2 dan seterusnya**

- Dokumen Inventarisasi Sistem Elektronik (SE)
- Dokumen Kategorisasi Sistem Elektronik (SE)
- Dokumen Identifikasi Infrastruktur Informasi Vital (IIV)

PERSYARATAN INDIKATOR 11

BADAN SIBER DAN SANDI NEGARA

INDIKATOR 11

Tingkat Kematangan Penerapan Kriptografi untuk Keamanan Data

NILAI IKASANDI PADA AREA KEMATANGAN PERSANDIAN

Syarat pemenuhan untuk **Level 5**

Nilai IKASANDI pada area Kematangan Persandian 4,00 ≤ IKASANDI ≤ 5,00

PENERAPAN KRIPTOGRAFI

Data Dukung untuk **Level 1 s.d Level 5**

Laporan/Dokumentasi Penerapan Kriptografi

PERSYARATAN INDIKATOR 12

BADAN SIBER DAN SANDI NEGARA

INDIKATOR 12

Tingkat Kematangan Kapabilitas Penanganan Insiden Siber

NILAI IKASANDI PADA AREA PENANGANAN INSIDEN SIBER

Hasil *self assessment*/yang telah diverifikasi

- **Level 1:** Nilai IKASANDI pada area Penanganan Insiden Siber 0 ≤ IKASANDI < 1,50
- **Level 2:** Nilai IKASANDI pada area Penanganan Insiden Siber 1,50 ≤ IKASANDI < 2,50

Hasil yang telah diverifikasi

- **Level 3:** Nilai IKASANDI pada area Penanganan Insiden Siber 2,50 ≤ IKASANDI < 3,50
- **Level 4:** Nilai IKASANDI pada area Penanganan Insiden Siber 3,50 ≤ IKASANDI < 4,00
- **Level 5:** Nilai IKASANDI pada area Penanganan Insiden Siber 4,00 ≤ IKASANDI ≤ 5,00

STATUS PEMBENTUKAN TIM TANGGAP INSIDEN SIBER (TTIS)

Data Dukung untuk **Level 2 dan seterusnya**

- Surat Tanda Register (STR) dan melihat pada masa berlaku STR tersebut

INVENTARISASI SE

BADAN SIBER DAN SANDI NEGARA

Pentingnya Inventarisasi SE

Visibilitas Penuh

Mengetahui objek yang dilindungi sbg awal langkah Keamanan

Kepatuhan Regulasi

Adanya kewajiban Penyelenggara Sistem Elektronik [PSE] agar menyelenggarakan Sistem Elektronik [SE] secara aman dan handal (termaktub pada beberapa dasar hukum seperti UU ITE, UU PDP, PP 71 PSTE, Perpres SPBE)

Optimalisasi Sumber Daya

Efisiensi dan efektivitas dengan fokus pada objek yang dijaga

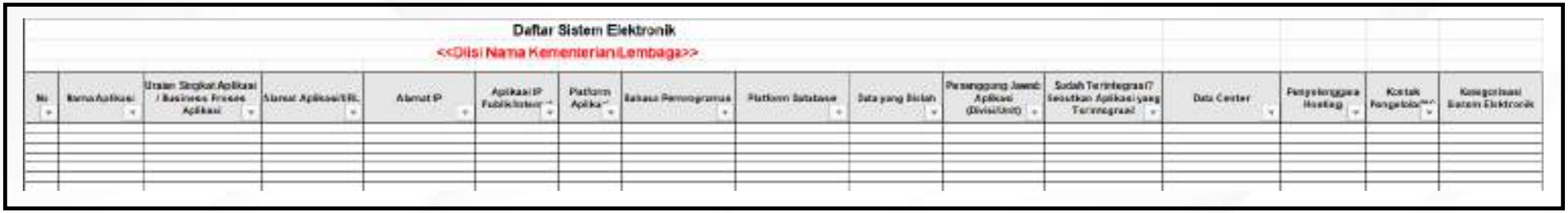
Kecepatan Respon

Mempercepat waktu deteksi dan pemulihan Ketika terjadi serangan siber

INVENTARISASI SE

BADAN SIBER DAN SANDI NEGARA

Form Inventarisasi SE



Daftar Sistem Elektronik

<<Diisi Nama Kementerian/Lembaga>>

No	Nama Aplikasi	Uraian Singkat Aplikasi / Business Proses Aplikasi	Alamat Aplikasi/URL	Alamat IP	Aplikasi IP Publik/Internal	Platform Aplikasi	Bahasa Pemrograman	Platform Database	Data yang Diolah	Penanggung Jawab Aplikasi (Divisi/Unit)	Sudah Terintegrasi? Sebutkan Aplikasi yang Terintegrasi	Data Center	Penyelenggara Hosting	Kontak Pengelola	Kategorisasi Sistem Elektronik

Nomor	nomor urut pendataan aset yang diidentifikasi
Nama Aplikasi	nama aplikasi/sistem elektronik yang dimiliki oleh instansi
Uraian Singkat Aplikasi	penjelasan terkait fungsi dari aplikasi
Alamat Aplikasi/URL	alamat website dari aplikasi (jika berbasis web)
Alamat IP	ip publik/ip lokal dari aplikasi
Aplikasi IP Publik/Internal	penggunaan aplikasi apakah bersifat publik atau internal
Platform Aplikasi	infrastruktur perangkat yang digunakan untuk menjalankan aplikasi (berbasis web/mobile)
Bahasa Pemrograman	bahasa yang digunakan untuk memberikan instruksi kepada aplikasi
Platform Database	platform/aplikasi yang digunakan untuk mengelola database
Data yang Diolah	data yang dikelola/disimpan/dikirimkan oleh aplikasi
Penanggung Jawab Aplikasi	unit kerja yang bertanggung jawab terhadap pengelolaan aplikasi
Aplikasi yang Terintegrasi	aplikasi lain yang terintegrasi
Data Center	Apakah aplikasi terhubung dengan PDN/PDNS atau memiliki Data Center sendiri
Penyelenggara Hosting	penyedia web hosting yang mengakomodir sistem elektronik yang dimiliki (misal niagahoster, idwebhost, siteground, dll)
Kategorisasi SE	kategori dari sistem elektronik berdasarkan hasil penilaian mandiri yang telah diverifikasi

BADAN SIBER DAN SANDI NEGARA

KATEGORI SE

KATEGORI	DESKRIPSI	SKOR
STRATEGIS	Sistem Elektronik strategis merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan Publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.	36-50
TINGGI	Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu	16-35
RENDAH	Merupakan Sistem Elektronik lainnya yang tidak termasuk STRATEGIS dan TINGGI	10-15

Bobot Nilai dari Setiap Jawaban Pertanyaan

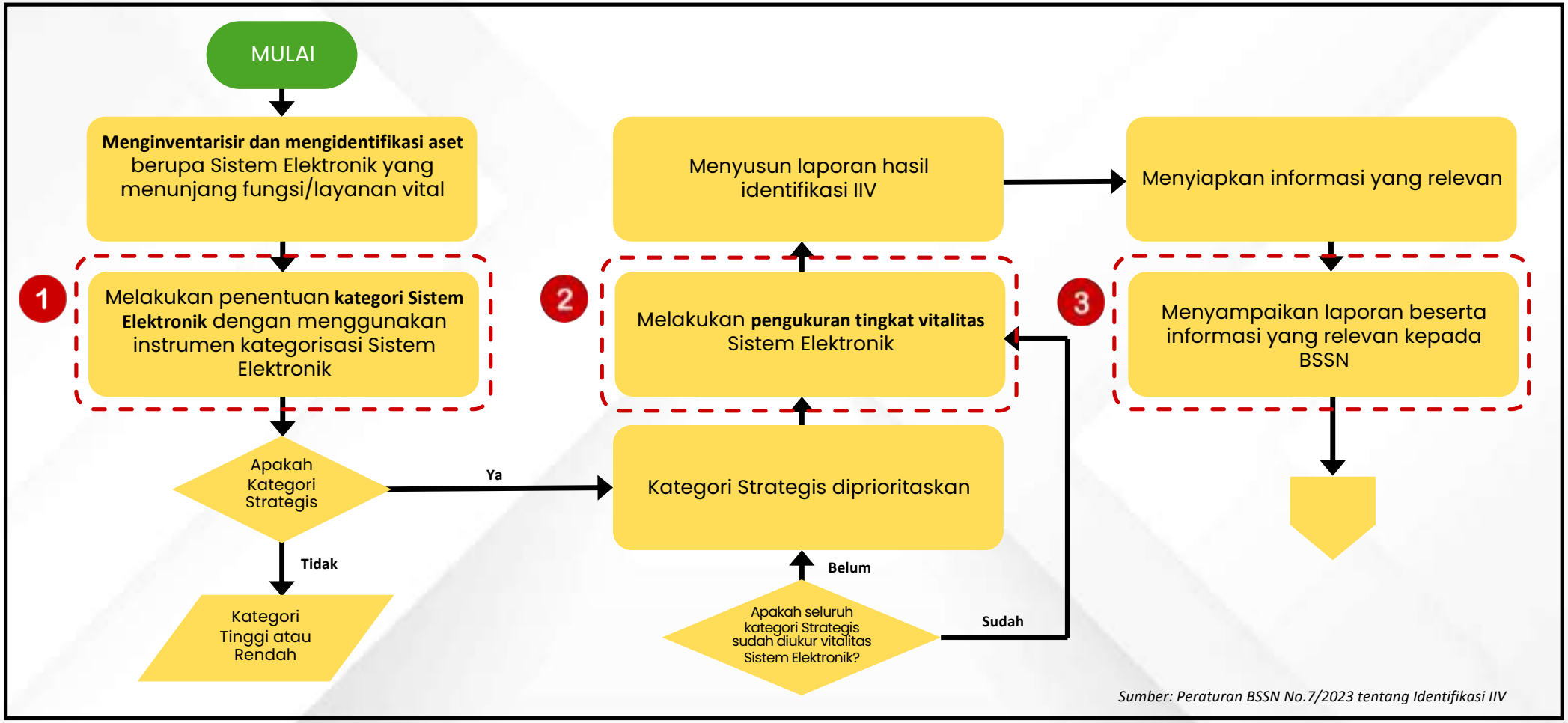
Status	Bobot Nilai
A	5
B	2
C	1

Referensi:

a. Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan SE
b. Peraturan BSSN Nomor 8 Tahun 2021 tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 Menggunakan Indeks KAMI
c. Peraturan BSSN Nomor 9 Tahun 2021 tentang Perubahan atas Peraturan BSSN Nomor 8 Tahun 2021

#	Karakteristik Instansi/Perusahaan
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih
1.10	Potensi kerugian atau dampak negatif dari insiden diterbitkannya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)

PROSEDUR IDENTIFIKASI IIV

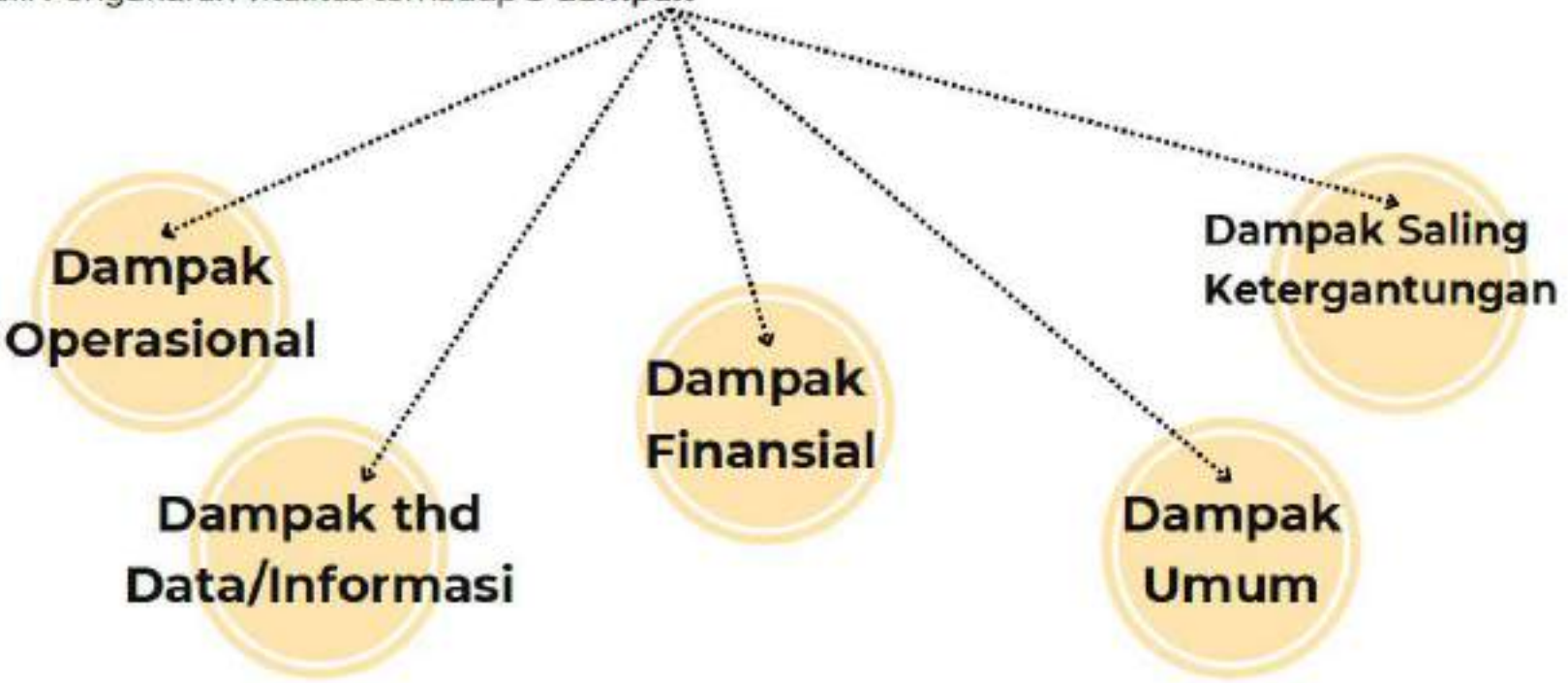


Sumber: Peraturan BSSN No.7/2023 tentang Identifikasi IIV

PROSEDUR IDENTIFIKASI IIV

BADAN SIBER DAN SANDI NEGARA

SE yang strategis dan tinggi diprioritaskan untuk dilanjutkan ke tahap pengukuran vitalitas dengan mengukur dampak-dampak yang mungkin terjadi jika SE tersebut terjadi gangguan/rusak/datanya bocor, dll. Pengukuran vitalitas terhadap **5 dampak**



Sumber: Peraturan BSSN No.7/2023 tentang Identifikasi IIV

Instrumen Pengukuran Kematangan Keamanan Siber dan Sandi (IKASANDI)

IKASANDI

DEFINISI

IKASANDI merupakan instrumen yang digunakan untuk mengukur Tingkat Kematangan Keamanan Siber dan Sandi sebuah organisasi atau Penyelenggara Sistem Elektronik [PSE].
Instrumen IKASANDI memiliki dua bagian pengukuran, yaitu Pengukuran Tingkat Kematangan Keamanan Siber dan Pengukuran Tingkat Kematangan Persandian.

TUJUAN

Kontrol yang diberikan diharapkan dapat digunakan sebagai panduan bagi PSE guna memenuhi kondisi penyelenggaraan SE secara aman dan handal melalui cerminan tingkat kematangan keamanan siber dan sandi

PIHAK YANG TERLIBAT

- Kementerian/Lembaga → PSE
- BSSN → asistensi dan verifikasi

AREA PENGUKURAN KEMATANGAN

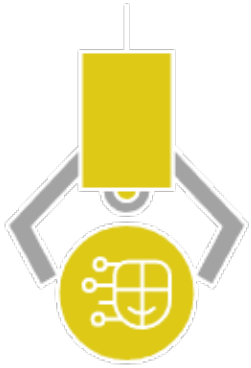
Kontrol Kematangan Keamanan Siber

Kontrol Persandian

Indeks Pemdigi

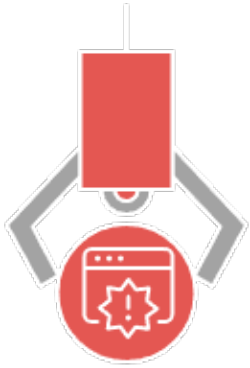
Penanganan Insiden

IKASANDI V2



Dashboard Keamanan Siber

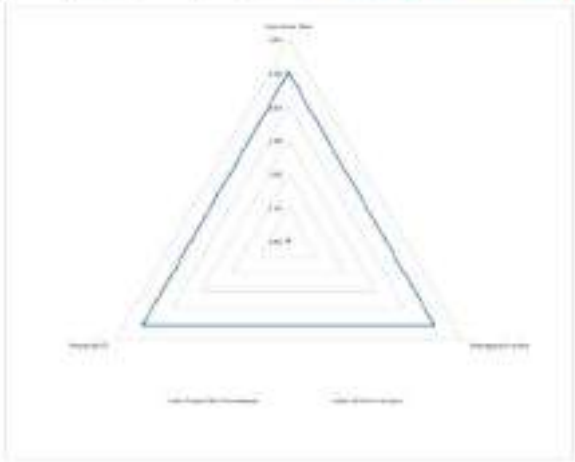
Dashboard Persandian



Dashboard Penanganan Insiden

Indeks Pemdigi

Kematangan Domain yang Diukur	Target Nilai Kematangan	Nilai Kematangan	Kategori Tingkat Kematangan
Keamanan Siber	2,51	0,00	[illegible]
Penanganan Insiden	2,51	0,00	[illegible]
Persandian	2,51	0,00	[illegible]



Tingkat Kematangan Penanganan Insiden Kategori SE: Strategis	2026							Kategori Tingkat Kematangan Penanganan Insiden
	Target Nilai Kematangan	Nilai Kematangan	Nilai Kematangan per-Domain	Seberan Nilai Indeks				
				0	1	2	3	4	5	
Total	2,51	0,00								Level 1 - Awal

No. IV Fase	Target	Nilai Kematangan			Nilai Maksimal	Seberan Indeks						Total
		Rendah	Tinggi	Tercapai		0	1	2	3	4	5	
Persiapan	2,51	0,00	0,00	0,00	5,00	26	0	0	0	0	0	26
Penanganan	2,51	0,00	0,00	0,00	5,00	18	0	0	0	0	0	18
[illegible]	2,51	0,00	0,00	0,00	5,00	9	0	0	0	0	0	9
TOTAL		0,00	0,00	0,00	TOTAL	53	0	0	0	0	0	

BADAN SIBER DAN SANDI NEGARA

SEBARAN KONTROL

KATEGORI SE

	RENDAH	TINGGI	STRATEGIS
Kontrol Kamsiber	**96**	**163**	**177**
> Kontrol Identifikasi	31	56	59
> Kontrol Proteksi	52	75	79
> Kontrol Deteksi	4	9	12
> Kontrol Gulih	9	23	27
Kontrol Persandian	**40**	**40**	**40**
> Irisan Kontrol Keamanan Siber dan Persandian	22	27	27
TOTAL	**114**	**176**	**190**

with great responsibility comes great obligations

BADAN SIBER DAN SANDI NEGARA

KARAKTERISTIK KONTROL

- Pengisian sesuai dengan kategori SE [**isi hanya kontrol warna**]
- Untuk Persandian, beberapa (irisan) terhubung dengan control kamsiber

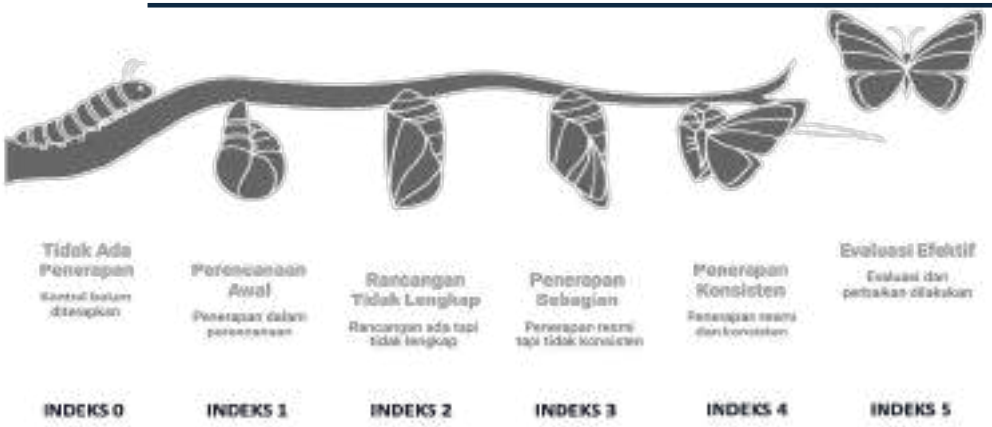
KATEGORI SE RENDAH

KATEGORI SE TINGGI

KATEGORI SE STRATEGIS

BADAN SIBER DAN SANDI NEGARA

RENTANG KONTROL DAN LEVEL KEMATANGAN IKASANDI



*Setiap kontrol pada instrumen akan ditanyakan implementasinya dalam bentuk indeks dengan rentang mulai dari indeks 0 hingga 5

*Setiap kontrol pada instrumen yang sudah dijawab akan menghasilkan nilai keseluruhan dalam bentuk leveling dengan rentang level 1 hingga 5

Level 1 (Awal)	Level 2 (Berulang)	Level 3 (Terdefinisi)	Level 4 (Terkelola)	Level 5 (Inovatif)
Indeks 0 - 1.50	Indeks 1.51 – 2.50	Indeks 2.51 – 3.50	Indeks 3.51 – 4.50	Indeks 4.51 – 5
1. Menggambarkan kondisi penerapan Keamanan Siber dan Sandi dalam tahap implementasi awal 2. Penerapan Keamanan Siber dan Sandi belum memiliki prosedur yang terorganisir 3. Penerapan Keamanan Siber dan Sandi bersifat informal 4. Keamanan Siber dan Sandi tidak dilakukan secara konsisten dan berkelanjutan 5. Dokumen manajemen risiko dan dokumen kontrol belum disusun	1. Menggambarkan kondisi penerapan Keamanan Siber dan Sandi dalam tahap implementasi yang berulang 2. Penerapan Keamanan Siber dan Sandi sudah memiliki prosedur yang terorganisir 3. Penerapan Keamanan Siber dan Sandi bersifat informal 4. Keamanan Siber dilakukan secara berulang namun belum konsisten dan belum berkelanjutan 5. Dokumen manajemen risiko dan dokumen kontrol sudah disusun namun belum ditetapkan	1. Menggambarkan kondisi penerapan Keamanan Siber dan Sandi dalam tahap implementasi yang telah terdefinisi dengan baik 2. Penerapan Keamanan Siber dan Sandi telah terorganisir dengan jelas 3. Penerapan Keamanan Siber dan Sandi bersifat formal 4. Keamanan Siber dan Sandi dilakukan secara berulang dan konsisten serta direviu secara berkala 5. Dokumen manajemen risiko dan dokumen kontrol sudah disusun dan sudah ditetapkan	1. Menggambarkan kondisi penerapan Keamanan Siber dan Sandi dalam tahap implementasi yang telah terkelola dengan baik 2. Penerapan Keamanan Siber dan Sandi telah terorganisir dengan baik namun belum dilakukan proses otomatisasi 3. Penerapan Keamanan Siber dan Sandi bersifat formal 4. Keamanan Siber dan Sandi dilakukan secara berulang dan implementasi perbaikan dilakukan berkelanjutan 5. Dokumen manajemen risiko dan dokumen kontrol sudah disusun dan sudah ditetapkan	1. Menggambarkan kondisi penerapan Keamanan Siber dan Sandi telah diimplementasikan secara optimal 2. Penerapan Keamanan Siber dan Sandi telah terorganisir dengan baik dan telah dilakukan proses otomatisasi 3. Penerapan Keamanan Siber dan Sandi bersifat formal 4. Keamanan siber dan sandi dilakukan secara berulang dan konsisten serta telah terintegrasi 5. Keamanan siber dan sandi menjadi bagian budaya organisasi secara menyeluruh 6. Dokumen manajemen risiko dan dokumen kontrol sudah ditetapkan


"Ingatlah bahwa kechilafan satu orang sahaja
tjukup sudah menjebabkan keruntuhan negara."
dr. Roebiono Kertopati
BAPAK PERSANDIAN INDONESIA