



SOSIALISASI SISTEM MANAJEMEN KEAMANAN INFORMASI

DIREKTORAT KEAMANAN SIBER DAN SANDI PEMERINTAHAN DASAR
OKTOBER 2022



Keamanan Siber | Komunikasi | Manajemen | Organisasi | Hukum | Teknologi | Pendidikan





Ivan Bashofi, S.ST.TP., M.T.

[CEH, ECSSA, LPT Master, CCNA, Anesor BNSP]

Sandiman Ahli Muda

Badan Siber dan Sandi Negara



Badan Siber dan Sandi Negara

www.bssn.go.id

021-52000000

Outline

Profil KSS Kab Tabalong

01



Standar Keamanan Informasi

02



- Keluarga ISO 27000
- Penerapan ISMS Sesuai ISO 27001
- Terbit 4 2022

Kewajiban IPPD

03



- Integrasi Dengan Kebijakan
- Fundamental Kewajiban PSE

Indeks KAMI

04



- Domain Pembelian Indeks KAMI



BADAN SIBER
DAN SANDI
NEGARA

**PROFIL KEAMANAN
SIBER DAN SANDI
KAB TABALONG**

**STANDAR
KEAMANAN
INFORMASI**





STANDAR KEAMANAN INFORMASI ???

SISTEM MANAJEMEN KEAMANAN INFORMASI ???

**Terminology**

Contoh: Istilah yang digunakan dalam standar untuk menjelaskan istilah yang digunakan dalam ISO 27000 untuk memastikan bahwa semua orang memahami dan berbicara tentang hal yang sama.

Requirements

Contoh: Persyaratan yang harus dipenuhi untuk memastikan bahwa sistem informasi yang dikembangkan memenuhi semua persyaratan yang ditetapkan.

Guidelines

Contoh: Petunjuk yang harus diikuti untuk memastikan bahwa sistem informasi yang dikembangkan memenuhi semua persyaratan yang ditetapkan.

See for Specifics

Contoh: Referensi ke standar lain yang relevan untuk memastikan bahwa sistem informasi yang dikembangkan memenuhi semua persyaratan yang ditetapkan.

FL

ISO 27000 Family of Standards

Introduction

ISO 27000

Requirements

ISO 27001

ISO 27002

ISO 27003

ISO 27004

Guidelines

ISO 27005

ISO 27006

ISO 27007

ISO 27008

ISO 27009

See for Specifics

ISO 27010

ISO 27011

ISO 27012

ISO 27013

ISO 27014

Contoh: <https://www.iso.org/standards/iso-27000-family-of-standards>
<https://www.iso.org/standards/iso-27000-family-of-standards>

Salah satu standar ISO 27000 family yang sudah dipublikasikan terkait "keamanan informasi, keamanan siber, dan perlindungan data pribadi" sebanyak 10 standar.

PENERAPAN SMKI

ISO 27001 merupakan suatu standar internasional untuk menerapkan Sistem Manajemen Keamanan Informasi.



SESUAI ISO 27001

ISO 27001 memberikan perlindungan terhadap informasi dengan menjamin kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability).

Dengan menerapkan ISO 27001, organisasi dapat mengelola risiko keamanan informasi secara efektif dan memastikan bahwa manajemen keamanan informasi yang baik.





REPUBLIC OF INDONESIA
MINISTRY OF COMMUNICATIONS AND INFORMATICS

DEPARTMENT OF INFORMATION SYSTEMS

SECRETARY

REPUBLIC OF INDONESIA
MINISTRY OF COMMUNICATIONS AND INFORMATICS
DEPARTMENT OF INFORMATION SYSTEMS
SECRETARY

SECRETARY OF THE DEPARTMENT

SECRETARY OF THE DEPARTMENT

Background: The Department of Information Systems is responsible for the development and implementation of information systems in the Ministry of Communication and Informatics. The Department is currently working on the development of the National Information System (NIS) and the National Information System (NIS) is a key component of the NIS. The Department is currently working on the development of the NIS and the NIS is a key component of the NIS.

Background: The Department of Information Systems is responsible for the development and implementation of information systems in the Ministry of Communication and Informatics. The Department is currently working on the development of the National Information System (NIS) and the National Information System (NIS) is a key component of the NIS. The Department is currently working on the development of the NIS and the NIS is a key component of the NIS.

PERBAN BSSN 4 TAHUN 2021

Perban ini terdiri dari 36 Pasal yang meliputi kebijakan Manajemen Keamanan Informasi dan Standar Teknik Prosedur Keamanan SPSS dengan ketentuan sebagai berikut:

- BAB I – Ketentuan Umum (Pasal 1)
- BAB II – Manajemen Keamanan Informasi SPSS (Pasal 2 – 10)
- BAB III – Standar Teknik dan Prosedur Keamanan SPSS (Pasal 11- 35)
- BAB IV – Penutup (Pasal 36)



KONSIDERAN

Perpres 95 Tahun 2018

telah untuk melaksanakan ketentuan Pasal 41 ayat (4) dan Pasal 48 ayat (2) Peraturan Presiden Nomor 10 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Menteri Komunikasi dan Informatika tentang Manajemen dan Standar Keamanan SPSS;



PILAR MANAJEMEN DAN STANDAR KEAMANAN SPBE





BAB II. MANAJEMEN KEAMANAN INFORMASI SPBE



PENETAPAN RUANG LINGKUP

PENETAPAN PENANGGUNG JAWAB

PERENCANAAN

DUKUNGAN PENGOPERASIAN

EVALUASI KINERJA

PERBAIKAN BERKELANJUTAN

BAB 11. MANAJEMEN KEAMANAN INFORMASI SPBE

PENETAPAN RUANG LINGKUP

Arahan yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE sebagaimana dimaksud paling sedikit meliputi:

- Data dan informasi SPBE;
- Aplikasi SPBE;
- Aset Infrastruktur SPBE; dan
- Kebijakan keamanan informasi SPBE yang telah dimiliki,



PENETAPAN PENANGGUNG JAWAB

KOORDINATOR SPBE

WAKIL PUSAT
SEKRETARIS AUL

WAKIL DAERAH
SEKRETARIS DAERAH



PELAKSANA TEKNIK KEAMANAN SPBE

a. Pejabat pimpinan tinggi pertama yang melaksanakan tugas dan fungsi di bidang keamanan TIK internal organisasi; dan
b. Pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara dan/atau mengembangkan Aplikasi SPBE.



PERENCANAAN

Program kerja Keamanan SPBE yang disusun berdasarkan tanggung jawab Keamanan SPBE dan target, melalui program kerja Keamanan SPBE.

Program kerja Keamanan SPBE sebagai acuan dan matriks paling rendah meliputi:

- Evaluasi Keamanan Keamanan SPBE;
- Pemetaan kerentanan Keamanan SPBE;
- Peningkatan Keamanan SPBE;
- Penanganan insiden Keamanan SPBE; dan
- Audit Keamanan SPBE.

DUKUNGAN PENGOPERASIAN

Dukungan pengoperasian paling rendah berupa:

- sumber daya manusia Keamanan SPBE; dan
- anggaran Keamanan SPBE.

EVALUASI KINERJA

- Evaluasi kinerja dilakukan terhadap pelaksanaan Manajemen Keamanan SPBE dan penerapan standar Keamanan SPBE;
- Evaluasi kinerja dilakukan oleh koordinator SPBE Instansi Pusat dan koordinator Pemerintah Daerah paling rendah 1 (satu) kali dalam 1 (satu) tahun.

PERSIAPAN BERKELANJUTAN

Persiapan berkelanjutan meliputi tindak lanjut dari hasil evaluasi kinerja.



BAB II. STANDAR KEAMANAN SPBE



STANDAR KEAMANAN APLIKASI SPBE

STANDAR KEAMANAN PUSAT DATA NASIONAL

STANDAR KEAMANAN DATA & INFORMASI

STANDAR KEAMANAN SISTEM PENGIKHTUNG LAYANAN

STANDAR KEAMANAN JARINGAN INTRA



SECURITY CONTROL/ MINIMUM REQUIREMENTS

DATA & INFORMASI

- Penerapan Enkripsi
- Penerbitan Sertifikat Elektronik
- Pemulihan & pencadangan

APLIKASI SPDC



Aplikasi Berbasis Web

- autentikasi;
- manajemen sesi;
- penerapan kontrol akses;
- validasi input;
- kriptografi pada verifikasi static;
- penanganan error dan penanganan log;
- proteksi data;
- keamanan komunikasi;
- pengendalian kode berbahaya;
- logikalisasi;
- file;
- keamanan API dan web service; dan
- keamanan konfigurasi.



Aplikasi Berbasis mobile

- penyimpanan data dan penyerasan privasi;
- kriptografi;
- autentikasi dan manajemen sesi;
- komunikasi jaringan;
- interaksi platform;
- kualitas kode dan pengaturan built; dan
- ketahanan





SECURITY CONTROL/ MINIMUM REQUIREMENTS

PUSAT DATA

Standar Keamanan Pusat Data SPBE terdiri dari:

- persyaratan keamanan fisik; dan
- persyaratan kondisi perangkat ke pusat data.

Persyaratan keamanan fisik Pusat Data mengacu pada SNI, khususnya keamanan:

- lokasi;
- kontrol akses;
- konstruksi;
- perangkat pengamanan dan pendukung; dan
- pengkabelan.

Contoh Persyaratan Pusat Data

- menempatkan server pemertara saat client mengakses server database dalam rangka pemeliharaan;
- memastikan perangkat komputer Pusat Data Nasional terbebas dari virus dan malware;
- memastikan setiap perangkat yang akan terkoneksi ke infrastruktur Pusat Data Nasional menggunakan IP address dan hostname yang telah ditentukan.





SECURITY CONTROL/ MINIMUM REQUIREMENTS

SISTEM PENYHUBUNG LAYANAN

Kecamatan Sistem Penghubung Layanan (SPL) meliputi:

- keamanan interoperabilitas data dan informasi;
- penerapan kontrol sistem integrasi;
- penerapan kontrol perangkat integrator;
- keamanan API dan web service;
- dan/atau
- ketentuan migrasi data.



JARINGAN INTRA

Kecamatan Jaringan Intra (JIP/JIPD) meliputi:

- aspek administrasi keamanan Jaringan Intra;
- kontrol akses dan autentikasi;
- persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
- kontrol keamanan gateway;
- kontrol keamanan access point pada jaringan nirkabel;
- kontrol konfigurasi access point pada jaringan nirkabel.



KEWAJIBAN IPPD



INTEGRASI DENGAN KEBIYAKAN

PP
TU 2018

Pengembangan Sistem dan
Transaksi Elektronik

Peraturan
B1/2018

Sistem Pemerintahan
Berbasis Elektronik

Peraturan
B1/2018

Sistem Pemerintahan dalam
Pengembangan Sistem
Elektronik

Tugas 1

- 1) Pengembangan Sistem Elektronik harus meliputi:
- a. analisis dan pengujian desain sistem;
 - b. analisis dan pengujian keamanan sistem;
 - c. analisis dan pengujian kinerja sistem;
 - d. analisis dan pengujian sistem yang akan dikembangkan.

Tugas 2

- a. Pengembangan Sistem Elektronik yang meliputi:
 1. analisis dan pengujian desain sistem;
 2. analisis dan pengujian keamanan sistem;
 3. analisis dan pengujian kinerja sistem;
 4. analisis dan pengujian sistem yang akan dikembangkan.
- b. Pengembangan Sistem Elektronik yang meliputi:
 1. analisis dan pengujian desain sistem;
 2. analisis dan pengujian keamanan sistem;
 3. analisis dan pengujian kinerja sistem;
 4. analisis dan pengujian sistem yang akan dikembangkan.
- c. Pengembangan Sistem Elektronik yang meliputi:
 1. analisis dan pengujian desain sistem;
 2. analisis dan pengujian keamanan sistem;
 3. analisis dan pengujian kinerja sistem;
 4. analisis dan pengujian sistem yang akan dikembangkan.

Tugas 3

- 1) Analisis dan Pengujian Desain Sistem yang akan dikembangkan.



WILEYJOURNAL

WILEYJOURNAL

WILEYJOURNAL

Tugas 4

- 1) Pengembangan Sistem Elektronik harus meliputi:
- a. analisis dan pengujian desain sistem;
 - b. analisis dan pengujian keamanan sistem;
 - c. analisis dan pengujian kinerja sistem;
 - d. analisis dan pengujian sistem yang akan dikembangkan.

- 1) Pengembangan Sistem Elektronik harus meliputi:
- a. analisis dan pengujian desain sistem;
 - b. analisis dan pengujian keamanan sistem;
 - c. analisis dan pengujian kinerja sistem;
 - d. analisis dan pengujian sistem yang akan dikembangkan.

- 1) Pengembangan Sistem Elektronik harus meliputi:
- a. analisis dan pengujian desain sistem;
 - b. analisis dan pengujian keamanan sistem;
 - c. analisis dan pengujian kinerja sistem;
 - d. analisis dan pengujian sistem yang akan dikembangkan.



ARAHAN MENTERI DALAM NEGERI

KEPUTUSAN MENTERI DALAM NEGERI
REPUBLIC OF INDONESIA
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020



KEPUTUSAN MENTERI DALAM NEGERI
REPUBLIC OF INDONESIA

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

Menyatakan bahwa
Penerapan Peraturan Menteri Kesehatan
No. 12/2020
Tentang
Penerapan Peraturan Menteri Kesehatan
No. 12/2020

- Penerapan Peraturan (SSN) Nomor 8 Tahun 2020 tentang Sistem Pengukuran dalam Penyelenggaraan Sistem Elektronik
- Penerapan Peraturan (SSN) Nomor 4 Tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis IT pada dan Keamanan SPBE
- Penerapan Standar Keamanan dan verifikasi standar keamanan dengan prioritas INI Biting Keminfo
- Penerapan Regulasi dan ketentuan keamanan informasi lainnya yang telah ditetapkan





PROVINSI

- IKK : Tingkat keamanan informasi pemerintah
- Rumus : $\frac{\text{Jumlah nilai per area keamanan informasi}}{\text{Jumlah area penilaian}} \times 100\%$

KABUPATEN/KOTA

- IKK : Tingkat keamanan informasi pemerintah
- Rumus : $\frac{\text{Jumlah nilai per area keamanan informasi}}{\text{Jumlah area penilaian}} \times 100\%$

Indikator Keamanan Informasi : Mengukur tingkat keamanan informasi pemerintah provinsi dan kabupaten/kota

Indikator :

Jumlah nilai per area keamanan informasi adalah jumlah hasil dari aspek keamanan informasi pemerintah provinsi dan kabupaten/kota yang diukur dengan menggunakan tingkat keparahan pelanggaran informasi di setiap aspeknya per aspek sesuai dengan 5 (lima) indikator utama program keamanan informasi pemerintah provinsi dan kabupaten/kota (struktur), dapat dikatakan bahwa ada enam aspek yang dinilai dalam aspek.

Indikator yang digunakan pengukuran yang dilaksanakan oleh aspek, program provinsi dan kabupaten/kota yang akan dinilai dalam aspek ini ada program keamanan informasi yang ada. Setelah melakukan informasi, penggunaan risiko keamanan informasi, manajemen risiko keamanan informasi, manajemen aset keamanan, manajemen kebijakan keamanan informasi, serta dari hasil penilaian dapat berupa laporan dan tindakan yang akan dilakukan untuk aspek yang dinilai oleh aspek.

Jumlah area penilaian adalah jumlah nilai keamanan (kekuatan) area penilaian yang ada. Setelah melakukan dengan melakukan pengukuran yang dilaksanakan oleh aspek, program provinsi dan kabupaten/kota yang akan dinilai dalam aspek ini ada program keamanan informasi.

CONTOH PERHITUNGAN INDIKATOR KINERJA KUNCI (IKK) URUSAN PERSANDIAN



PENGISIAN DATA IKK YANG BENAR

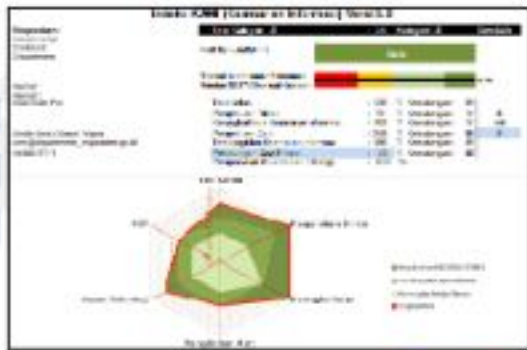
NO IKK	TEK Deskripsi	RUMUS	Data Data	
			Nilai Data	Uraian Nilai
1	Tingkat Keamanan Informasi Pemerintah	Jumlah nilai per area keamanan informasi	840	840/3
		Jumlah area penilaian	340	

PENGISIAN DATA IKK YANG SALAH

NO IKK	TEK Deskripsi	RUMUS	Data Data	
			Nilai Data	Uraian Nilai
1	Tingkat Keamanan Informasi Pemerintah	Jumlah nilai per area keamanan informasi	780	5.720/3
		Jumlah area penilaian	5	



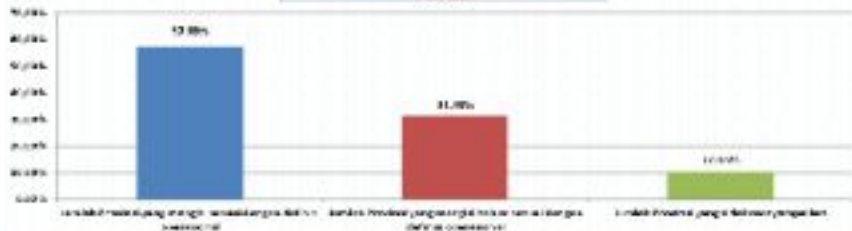
Sertifikat NCARW (lihat note)



REVIEW HASIL EVALUASI TERHADAP LPPD UTK URUSAN PERSANDIAN



Perwakilan pengisian KIR Tingkat Kabupaten Informasi
Kabupaten



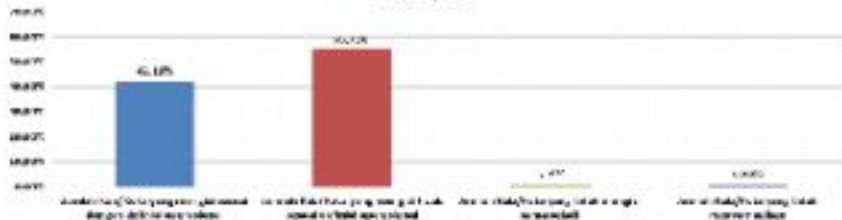
Jumlah KIR yang diisi secara mandiri dengan data diri	Jumlah KIR yang diisi dengan data diri dan data yang diberikan oleh instansi	Jumlah KIR yang diisi dengan data diri yang diberikan oleh instansi	Total
13	32	4	49



REVIEW HASIL EVALUASI TERHADAP LPPD UTK URUSAN PERSANDIAN



Persentase pengisian BUK (Buku Keabsahan) terhadap
Kebijakan/Kelembagaan



Jumlah kebijakan yang menjadi acuan dengan definisi yang jelas	Jumlah kebijakan yang menjadi acuan dengan definisi yang tidak jelas	Jumlah kebijakan yang menjadi acuan dengan definisi yang tidak jelas	Jumlah kebijakan yang menjadi acuan dengan definisi yang tidak jelas	Jumlah
2,8	2,8	1	1	6,18



İNDEKS KAMI



What ?

Alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di organisasi

Who ?

PSE yang memperniatkan penerapan
SN/ISO IEC 27001

How ?

Menggunakan Instrumen Indeks KAMI
yang dapat diunduh pada tautan :
<https://dan.go.id/indeks-kami/>

Where ?

Evaluasi dilakukan terhadap berbagai area
yang menjadi target penerapan
keamanan informasi dengan ruang
lingkup pembahasan yang memenuhi
aspek keamanan pada SN/ISO IEC 27001



Why ?

- ❑ Memberikan gambaran kondisi kesiapan kerangka kerja pengamanan informasi kepada pimpinan instansi terhadap Penerapan SN/ISO IEC 27001
- ❑ Sebagai sarana untuk meningkatkan kesadaran keamanan informasi dan peningkatan kesiapan SMI

When ?

Digunakan secara berkala sebagai alat dalam melakukan tinjauan ulang kesiapan keamanan informasi sekaligus mengukur keberhasilan inisiatif yang diterapkan



AREA EVALUASI (IKAMI v4.2)

Diagram ini menggambarkan siklus evaluasi program kesehatan masyarakat. Diagram ini menunjukkan siklus evaluasi program kesehatan masyarakat yang meliputi: perencanaan, pelaksanaan, monitoring, evaluasi, dan tindak lanjut. Diagram ini menunjukkan siklus evaluasi program kesehatan masyarakat yang meliputi: perencanaan, pelaksanaan, monitoring, evaluasi, dan tindak lanjut.

Diagram ini menggambarkan siklus evaluasi program kesehatan masyarakat. Diagram ini menunjukkan siklus evaluasi program kesehatan masyarakat yang meliputi: perencanaan, pelaksanaan, monitoring, evaluasi, dan tindak lanjut.

Diagram ini menggambarkan siklus evaluasi program kesehatan masyarakat. Diagram ini menunjukkan siklus evaluasi program kesehatan masyarakat yang meliputi: perencanaan, pelaksanaan, monitoring, evaluasi, dan tindak lanjut.

II. Tesis Kritis

Diagram ini menggambarkan siklus evaluasi program kesehatan masyarakat. Diagram ini menunjukkan siklus evaluasi program kesehatan masyarakat yang meliputi: perencanaan, pelaksanaan, monitoring, evaluasi, dan tindak lanjut.

III. Hukuk

Diagram ini menggambarkan siklus evaluasi program kesehatan masyarakat. Diagram ini menunjukkan siklus evaluasi program kesehatan masyarakat yang meliputi: perencanaan, pelaksanaan, monitoring, evaluasi, dan tindak lanjut.

IV. Kesehatan Kerja

Diagram ini menggambarkan siklus evaluasi program kesehatan masyarakat. Diagram ini menunjukkan siklus evaluasi program kesehatan masyarakat yang meliputi: perencanaan, pelaksanaan, monitoring, evaluasi, dan tindak lanjut.

V. Pengobatan

VI. Tindakan

VII. Supervisi

I. Konsep



PERUBAHAN versi 4.2 → versi 5.0

OKULTRAHUN 2021

INDEX KAMU v4.2

1. Kategori SE
2. Tata Kelola
3. Risiko
4. Kerangka Kerja
5. Pengelolaan Aset
6. Teknologi
7. Suplemen

Area Suplemen: Efektivitas Pihak Ketiga, Pengamanan Layanan Infrastruktur Aset, dan Pelindungan Data Privat

INDEX KAMU v5.0

1. Kategori SE
2. Tata Kelola
3. Risiko
4. Kerangka Kerja
5. Pengelolaan Aset
6. Teknologi
7. Pelindungan Data Privat
8. Suplemen

Pemindahan area evolusi sesuai ISO 27001:2022, pada Kerangka Kerja, Pengelolaan Aset, dan Teknologi

Demutuhan area evolusi Suplemen (Penggunaan Infrastruktur Layanan Aset) ke area evolusi utama (Pengelolaan Aset)

Pemisahan area evolusi Suplemen (Pelindungan Data Privat) menjadi area sendiri/terpisah

Area Suplemen: Pengamanan Efektivitas Pihak Ketiga, Pengamanan Layanan

Proses Penilaian IKAMI

Peraturan BSSN No.8 dan 9 Tahun 2021

- Penilaian aspek IKAMI, paling sedikit meliputi:
- Tata Kelola;
 - Pengelolaan Risiko;
 - Kerangka Kerja Keamanan;
 - Pengelolaan Data dan Teknologi & Informasi;
 - Suplemen.

- NDA (Perjanjian Kerahasiaan)
- Tahapan Verifikasi:
- Verifikasi kelengkapan dokumen kebijakan dan/atau prosedur; dan
 - Verifikasi penetapan dokumen kebijakan dan/atau prosedur.

- Sertifikat IKAMI
- bagian dari hasil
- kegiatan **SIPT** atau
- CIPT/CIPI**

Koordinasi

Bimtek

Penilaian Mandiri

Permohonan Verifikasi

Verifikasi

Penetapan Verifikasi

- Kelengkapan Dokumen:
- Draft permohonan;
 - Kelengkapan pengajuan verifikasi penilaian IKAMI;
 - Daftar dokumen dan dokumen;
 - IKAMI yang telah ditandatangani; dan
 - Informasi rinci tentang P2E.

- Laporan memuat:
- Tingkat kelengkapan P2E dalam menerapkan SIPT/CIPT/CIPI; dan
 - Dasar legal kebijakan, ketentuan dan rekomendasi seluruh aspek IKAMI.



**BADAN SIBER
DAN SANDI
NEGARA**



CONTOH FORMAT MKI SPBE



BADAN SIBER DAN SANDI NEGARA

Jalan Jenderal Sudirman Kav. 52-53, Jakarta Selatan 12131
 Telp. (021) 57170000, Faks (021) 57170001, 57170002
 E-mail: info@sisnib.go.id, sisnib@sisnib.go.id

Ditujukan : LEMBARAN TUGAS (LST) 002
 Tanggal : 10 Januari 2020
 Di : 100 Jendral Sudirman
 Subjek : Menyampaikan informasi tentang hasil analisis dan pengolahan data yang diperoleh dari sistem keamanan informasi (SI) yang terdapat di lingkungan instansi.

Pengantar

1. Menyampaikan informasi tentang hasil analisis dan pengolahan data yang diperoleh dari sistem keamanan informasi (SI) yang terdapat di lingkungan instansi.
2. Menyampaikan informasi tentang hasil analisis dan pengolahan data yang diperoleh dari sistem keamanan informasi (SI) yang terdapat di lingkungan instansi.

Di

1. Berdasarkan dasar hukum yang berlaku, khususnya Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP-71/2019), maka Badan Siber dan Sandi Negara (BSSN) memiliki tugas pokok dan fungsi sebagai berikut:

2. Berdasarkan dasar hukum yang berlaku, khususnya Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP-71/2019), maka Badan Siber dan Sandi Negara (BSSN) memiliki tugas pokok dan fungsi sebagai berikut:

Jakarta, 10 Januari 2020
 Kepala Badan Siber dan Sandi Negara
 (Sesuai dengan tugas pokok dan fungsi)

(Sesuai dengan tugas pokok dan fungsi)



KEPADA YAHYDI/KEPADA YAHYDI/KEPADA YAHYDI

KEPADA YAHYDI/KEPADA YAHYDI/KEPADA YAHYDI
 (Sesuai dengan tugas pokok dan fungsi)

(Sesuai dengan tugas pokok dan fungsi)

KEPADA YAHYDI/KEPADA YAHYDI/KEPADA YAHYDI
 (Sesuai dengan tugas pokok dan fungsi)

KEPADA YAHYDI/KEPADA YAHYDI/KEPADA YAHYDI

(Sesuai dengan tugas pokok dan fungsi)



Mayjen TNI Dr. Koediono Kertogati
(1914 - 1994)

Wapak Permandian Republik Indonesia

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

BERSAMA BSSN

NEGARA AMAN RAKYAT SEJAHTERA



TERIMA KASIH



bsn.go.id



kas.pemda@bsn.go.id



Jl. Raya Mochtar 70 Bojongsari



03285511

