Sistem Manajemen Keamanan Informasi

Sebuah pengantar dan hubungannya dengan SPBE

Pelatihan Virtual Indeks KAMI bagi SDM Aparatur Bidang Persandian dan Keamanan Informasi DISKOMINFO Kab/Kota Se Jawa Tengah T.A 2021

Kelompok Audit Keamanan Informasi, Direktorat Proteksi Pemerintah, BSSN

Dasar

Perpres 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

Permenpanrb 59 tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik

Perban BSSN no 4 tahun 2021 tentang Pedoman Manajemen Keamanan SPBE dan Standar Teknis & Prosedur Keamanan SPBE

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

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.

Permenpan no 59 tahun 2020

Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik

MENTERI
PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA

SALINAN

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,

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.

Perban BSSN no 4 tahun 2021

Pedoman Manajemen Keamanan SPBE

dan Standar Teknis & Prosedur Keamanan SPBE

21 July 2021

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;

Pedoman Manajemen Keamanan Informasi

21 July 2021

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.

Permendagri no 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

SISTEM MANAJEMEN KEAMANAN INFORMASI

ISO 27001:2013, Perban BSSN no 8 tahun 2020

SNI 27001 : Sistem Manajemen Keamanan Informasi

Merupakan bagian dari keselurahan sistem manajemen, berdasarkan **pendekatan risiko bisnis**, untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memeliharadan memperbaiki pengamanan informasi

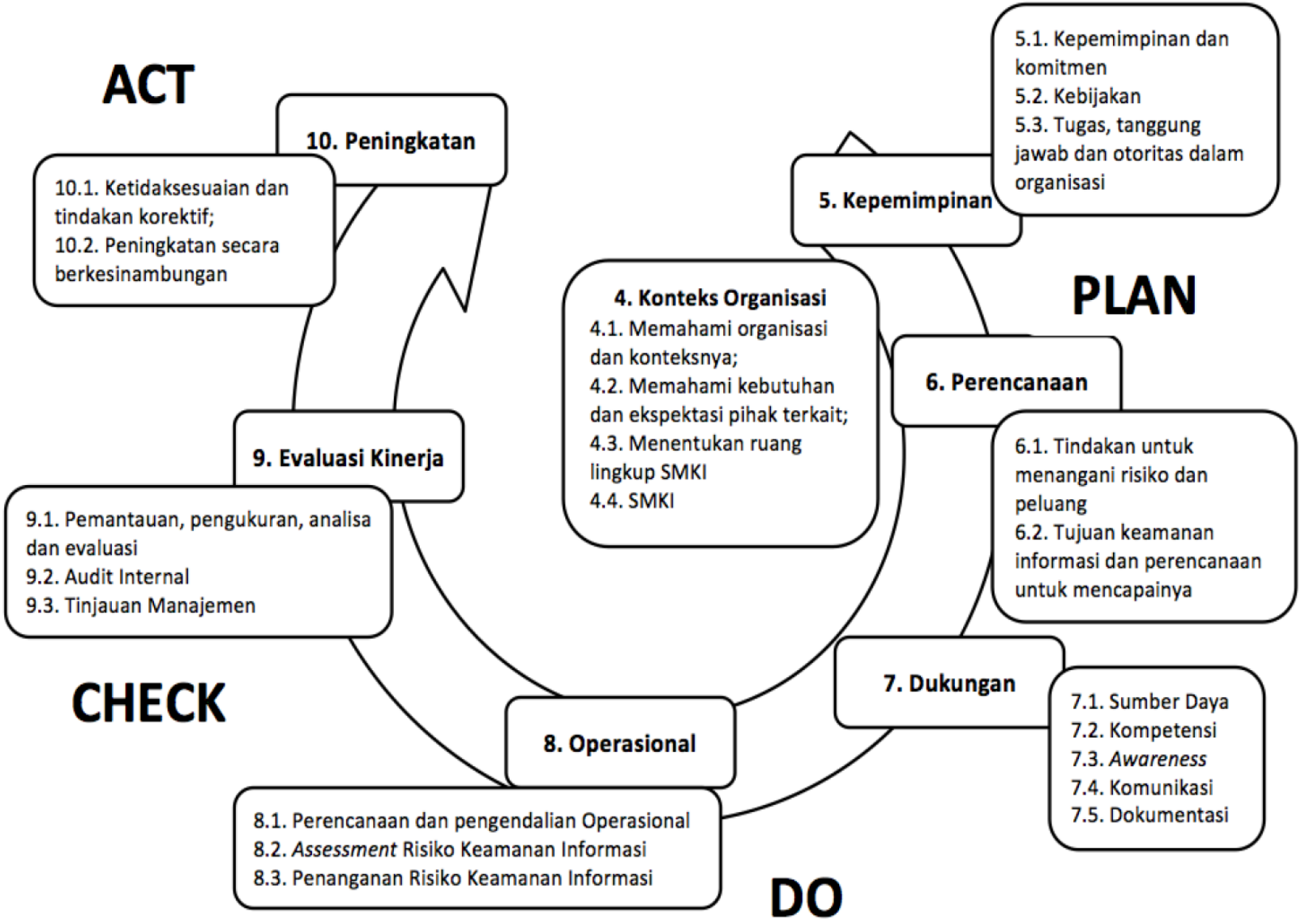
Lingkup dan Tujuan SNI/ISO 27001

- Mendefinisikan persyaratan untuk menetapkan, menerapkan, memelihara, meningkatkan secara berkesinambungan terhadap sistem manajemen keamanan informasi
- Persyaratan dalam standar ini bersifat umum dimaksudkan agar dapat diterapkan oleh organisasi tanpa membatasi jenis, ukuran, serta sifat organisasi
- Merupakan Standar dengan pendekatan berbasis resiko, artinya melibatkan asesmen serta manajemen resiko terkait keamanan informasi
- Merupakan standar internasional dengan sasaran melindungi informasi dalam kontek CIA (confidentiality, Integrity dan Availibility)

Manfaat penerapan SMPI

- Meningkatkan reputasi organisasi
- Meningkatkan kepercayaan stakeholder
- Pengelolaan insiden menjadi lebih baik
- Meningkatkan kualitas layanan
- Perbaikan respon time
- Perubahan proses reaktif menjadi proaktif
- Peningkatan berkelanjutan
- Mendukung proses bisnis

Struktur SNI ISO 27001:2013



Penentuan Ruang Lingkup

Hal hal yang perlu di perhatikan dalam menentukan ruang lingkup:

- Tujuan dari penerapan SMPI
- Implementasi SMPI apakah dalam satu unit kerja atau lebih
- Fasilitas terkait keberlangsungan bisnis dan pemulihan terhadap bencana (disaster recovery)
- Pemenuhan peraturan/perundang undangan / kewajiban
- Perlindungan terhadap asset yang strategis / penting
- Kepastian terhadap pemangku kepentingan terhadap perlindungan aset informasi
- Karakter bisnis proses, lokasi , aset dan teknologi

Penyusunan Kebijakan dan Prosedur SMPI

1. Strategi penerapan/implementasi SMKI sebaiknya dilakukan dengan menyelaraskan kegiatan yang sedang berlangsung di instansi/Lembaga.
2. Jika instansi/Lembaga sedang melakukan proyek pengembangan aplikasi, arahkan, dan damping agar setiap tahapan pengembangan aplikasi dapat mematuhi kebijakan dan prosedur yang telah ditetapkan yang antara lain mencakup:
   - ✓ Persetujuan investasi proyek (untuk proyek outsource atau kegiatan yang memerlukan anggaran);
   - ✓ Persyaratan keamanan aplikasi (syarat password minimum, session time-out, otentikasi, dan sebagainya)
   - ✓ Non Disclosure Agreement (perjanjian menjaga kerahasiaan untuk pihak ketiga)
   - ✓ Change management
   - ✓ Lisensi dan standar yang digunakan
3. Hasil penerapan SMKI harus dicatat dalam bentuk laporan, log, rekaman atau isian formulir yang relevan yang mendukung kebijakan atau prosedur yang ditetapkan seperti laporan pencatatan insiden dan penyelesaiannya, daftar pengguna aplikasi, log, aktivitas user, laporan pelatihan/sosialisasi, permintaan perubahan dan realisasinya, hasil pengujian aplikasi, laporan perawatan computer dan sebagainya.

Contoh Kebijakan SMPI

MENTERI KEUANGAN
REPUBLIK INDONESIA

SALINAN

KEPUTUSAN MENTERI KEUANGAN REPUBLIK INDONESIA

NOMOR 695/KMK.01/2017

TENTANG

KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN KEMENTERIAN KEUANGAN

MENTERI KEUANGAN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melindungi kerahasiaan, keutuhan, dan ketersediaan Aset Informasi Kementerian Keuangan dari berbagai bentuk gangguan serta ancaman keamanan informasi, perlu dilakukan pengelolaan keamanan Aset Informasi Kementerian Keuangan yang sesuai dengan SNI ISO/IEC 27001:2013;

SALINAN

GUBERNUR DAERAH ISTIMEWA YOGYAKARTA

PERATURAN GUBERNUR DAERAH ISTIMEWA YOGYAKARTA
NOMOR 31 TAHUN 2016
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR DAERAH ISTIMEWA YOGYAKARTA,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi di lingkungan Pemerintah Daerah Daerah Istimewa Yogyakarta dari berbagai ancaman keamanan informasi baik dari dalam maupun luar, perlu melakukan pengelolaan keamanan informasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Gubernur tentang Sistem Manajemen Keamanan Informasi;

“Kechilafan Satu Orang Sahaja Tjukup Sudah Menjebabkan Keruntuhan Negara”

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

TERIMA KASIH