PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2024
TENTANG
STANDAR DAN TATA CARA PELAKSANAAN AUDIT KEAMANAN
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 58 ayat (6) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik;

Mengingat :

1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
2. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
3. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 16 Tahun 2022 tentang Kebijakan Umum Penyelenggaraan Audit Teknologi Informasi dan Komunikasi (Berita Negara Republik Indonesia Tahun 2022 Nomor 1374);
4. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG STANDAR DAN TATA CARA PELAKSANAAN AUDIT KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna sistem pemerintahan berbasis elektronik.
2. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
3. Audit Keamanan SPBE adalah audit teknologi informasi dan komunikasi cakupan keamanan SPBE.
4. Audit Teknologi Informasi dan Komunikasi yang selanjutnya disebut Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
5. Badan Siber dan Sandi Negara yang selanjutnya disebut Badan adalah lembaga pemerintah yang melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi.
6. Instansi Pusat adalah kementerian, lembaga pemerintah non kementerian, kesekretariatan lembaga negara, kesekretariatan lembaga nonstruktural, dan lembaga pemerintah lainnya.
7. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
8. Lembaga Pelaksana Audit TIK yang selanjutnya disebut LATIK adalah lembaga yang melaksanakan Audit TIK.
9. LATIK Terakreditasi adalah badan hukum yang telah terakreditasi sebagai pelaksana Audit TIK.
10. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
11. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
12. Infrastruktur SPBE Nasional adalah Infrastruktur SPBE yang terhubung dengan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah dan digunakan secara bagi pakai oleh Instansi Pusat dan Pemerintah Daerah.
13. Peta Rencana SPBE adalah dokumen yang mendeskripsikan arah dan langkah penyiapan dan pelaksanaan SPBE yang terintegrasi.

14. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
15. Aplikasi Umum adalah Aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh Instansi Pusat dan/atau Pemerintah Daerah.
16. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh Instansi Pusat atau Pemerintah Daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan Instansi Pusat dan Pemerintah Daerah lain.
17. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
18. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
19. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
20. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
21. Infrastruktur Informasi Vital yang selanjutnya disingkat IIV adalah Sistem Elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional, baik berdiri sendiri maupun saling bergantung dengan Sistem Elektronik lainnya dalam menunjang sektor strategis, yang jika terjadi gangguan, kerusakan, dan/atau kehancuran pada infrastruktur dimaksud berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional.

BAB II
STANDAR AUDIT KEAMANAN SPBE

Bagian Kesatu
Umum

Pasal 2

Standar Audit Keamanan SPBE terdiri atas:
a. objek Audit Keamanan SPBE;
b. pelaksana Audit Keamanan SPBE;
c. kriteria Audit Keamanan SPBE;
d. bukti Audit Keamanan SPBE; dan
e. kesimpulan Audit Keamanan SPBE.

Bagian Kedua
Objek Audit Keamanan SPBE

Pasal 3

(1) Objek Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 2 huruf a terdiri atas:
    a. Infrastruktur SPBE Nasional;
    b. Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah;
    c. Aplikasi Umum; dan
    d. Aplikasi Khusus.
(2) Infrastruktur SPBE Nasional sebagaimana dimaksud pada ayat (1) huruf a terdiri atas:
    a. Pusat Data nasional;
    b. Jaringan Intra pemerintah; dan
    c. Sistem Penghubung Layanan pemerintah.
(3) Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah sebagaimana dimaksud pada ayat (1) huruf b terdiri atas:
    a. Jaringan Intra Instansi Pusat dan Pemerintah Daerah; dan
    b. Sistem Penghubung Layanan Instansi Pusat dan Pemerintah Daerah.
(4) Objek Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) termasuk keamanan data dan informasi yang dikelola di dalamnya.

Bagian Ketiga
Pelaksana Audit Keamanan SPBE

Pasal 4

(1) Pelaksana Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 2 huruf b yaitu LATIK cakupan Keamanan SPBE.
(2) LATIK cakupan Keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. LATIK pemerintah; atau
    b. LATIK Terakreditasi yang terdaftar.

Pasal 5

(1) LATIK pemerintah sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf a melaksanakan audit keamanan terhadap Infrastruktur SPBE Nasional dan Aplikasi Umum.
(2) LATIK pemerintah sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Badan.
(3) Audit keamanan sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 6

(1) LATIK Terakreditasi yang terdaftar sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf b harus:

a. terakreditasi oleh lembaga nonstruktural yang bertugas dan bertanggung jawab di bidang akreditasi lembaga penilaian kesesuaian; dan
b. terdaftar pada Badan.

(2) LATIK Terakreditasi yang terdaftar sebagaimana dimaksud pada ayat (1) melaksanakan Audit Keamanan SPBE terhadap Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah serta Aplikasi Khusus.

(3) LATIK Terakreditasi yang terdaftar dalam melaksanakan Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) membentuk tim auditor Keamanan SPBE.

(4) Dalam hal LATIK Terakreditasi yang terdaftar sebagaimana dimaksud pada ayat (1) belum ada, pelaksanaan Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) dilaksanakan oleh LATIK pemerintah.

(5) Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun.

Pasal 7

(1) Auditor Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) harus memiliki kompetensi Audit Keamanan SPBE yang terdiri atas:
a. latar belakang pendidikan;
b. keahlian dan pengalaman;
c. pengetahuan tentang standar Audit Keamanan SPBE;
d. pengetahuan umum tentang objek Audit Keamanan SPBE; dan
e. keterampilan yang memerlukan pengetahuan khusus dalam bidang tertentu sesuai dengan Audit Keamanan SPBE yang dilaksanakan.

(2) Bentuk kompetensi sebagaimana dimaksud pada ayat (1) dibuktikan dengan sertifikat kompetensi yang diterbitkan oleh lembaga yang berwenang dan masih berlaku.

(3) Dalam hal penyelenggara sertifikasi kompetensi sebagaimana dimaksud pada ayat (2) belum tersedia, kompetensi dibuktikan dengan dokumen lainnya yang berlaku dan menyatakan keahlian.

Pasal 8

(1) Pelaksanaan Audit Keamanan SPBE yang dilaksanakan oleh LATIK Terakreditasi sebagaimana dimaksud dalam Pasal 6 dikecualikan untuk Instansi Pusat tertentu.

(2) Pelaksanaan Audit Keamanan SPBE untuk Instansi Pusat tertentu sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Badan.

(3) Instansi Pusat tertentu sebagaimana dimaksud pada ayat (2) terdiri atas:
a. kementerian yang menyelenggarakan urusan pemerintahan di bidang kesekretariatan negara;

b. lembaga pemerintah yang menyelenggarakan tugas memberikan dukungan manajemen kabinet kepada Presiden dan Wakil Presiden;
c. kementerian yang menyelenggarakan urusan pemerintahan di bidang luar negeri;
d. kementerian yang menyelenggarakan urusan pemerintahan di bidang pertahanan;
e. Tentara Nasional Indonesia;
f. Kepolisian Negara Republik Indonesia;
g. Badan Intelijen Negara; dan
h. Instansi Pusat lain yang ditetapkan dengan Keputusan Kepala Badan.

(4) Penetapan Instansi Pusat lain sebagaimana dimaksud pada ayat (3) huruf h dilakukan berdasarkan usulan Instansi Pusat yang merupakan penyelenggara IIV.

Pasal 9

(1) Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) dilakukan pada Aplikasi Khusus dan Infrastruktur SPBE Instansi Pusat tertentu sebagaimana dimaksud dalam Pasal 8 ayat (3) yang ditetapkan sebagai IIV sesuai dengan ketentuan peraturan perundang-undangan.
(2) Dalam hal Aplikasi Khusus dan Infrastruktur SPBE Instansi Pusat tertentu tidak termasuk dalam IIV, Audit Keamanan SPBE dilaksanakan oleh LATIK Terakreditasi yang terdaftar.
(3) Audit Keamanan SPBE terhadap Aplikasi Khusus dan Infrastruktur SPBE Instansi Pusat tertentu sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun.

Bagian Keempat
Kriteria Audit Keamanan SPBE

Pasal 10

(1) Kriteria Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 2 huruf c meliputi hal pokok teknis pada:
a. tata kelola Keamanan SPBE;
b. manajemen Keamanan SPBE;
c. fungsionalitas dan kinerja Keamanan SPBE; dan
d. aspek keamanan lainnya.
(2) Hal pokok teknis sebagaimana dimaksud pada ayat (1) disusun dengan mempertimbangkan:
a. kebijakan makro terkait Keamanan SPBE dan pelindungan data pribadi; dan
b. kebijakan meso terkait Keamanan SPBE dan pelindungan data pribadi.
(3) Kebijakan makro dan kebijakan meso sebagaimana dimaksud pada ayat (2) merupakan kebijakan yang ditetapkan dalam peraturan perundang-undangan.
(4) Kriteria Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Kepala Badan.

Pasal 11

(1) Tata Kelola Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf a meliputi pemeriksaan atas aktivitas:
   a. evaluasi Keamanan SPBE;
   b. pengarahan Keamanan SPBE; dan
   c. pengendalian Keamanan SPBE.
(2) Evaluasi Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf a dilakukan untuk memeriksa mekanisme penilaian kinerja Keamanan SPBE yang dilakukan oleh organisasi sesuai dengan standar dan tujuan yang ditetapkan.
(3) Pengarahan Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf b dilakukan untuk memeriksa komitmen pimpinan dalam pengambilan keputusan dan pemberian arahan strategis Keamanan SPBE.
(4) Pengendalian Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf c dilakukan untuk memeriksa mekanisme pengawasan manajemen Keamanan SPBE yang dilakukan oleh organisasi sesuai dengan kebijakan dan prosedur yang ditetapkan.

Pasal 12

(1) Manajemen Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf b meliputi pemeriksaan terhadap tahapan:
   a. perencanaan Keamanan SPBE;
   b. pengembangan Keamanan SPBE;
   c. pengoperasian Keamanan SPBE; dan
   d. pemantauan Keamanan SPBE.
(2) Perencanaan Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf a dilakukan untuk memeriksa penetapan kebijakan dan prosedur Keamanan SPBE sesuai dengan manajemen risiko Keamanan SPBE dan kriteria Audit Keamanan SPBE.
(3) Pengembangan Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf b dilakukan untuk memeriksa pengembangan desain kendali keamanan yang sesuai dengan manajemen risiko Keamanan SPBE dan kriteria Audit Keamanan SPBE.
(4) Pengoperasian Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf c dilakukan untuk memeriksa implementasi prosedur dan kendali Keamanan SPBE.
(5) Pemantauan Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf d dilakukan untuk memeriksa pelaksanaan kegiatan Keamanan SPBE sesuai dengan rencana yang ditetapkan.

Pasal 13

(1) Pemeriksaan sebagaimana dimaksud dalam Pasal 12 ayat (1) dilakukan untuk memastikan penerapan pengendalian Keamanan SPBE yang terdiri atas:
   a. organisasi keamanan;
   b. keamanan personel;

c. keamanan fisik; dan
d. keamanan teknologi.

(2) Organisasi keamanan sebagaimana dimaksud pada ayat (1) huruf a merupakan struktur organisasi yang mendukung kebijakan dan prosedur Keamanan SPBE termasuk penetapan tanggung jawab dan wewenang manajemen Keamanan SPBE.

(3) Keamanan personel sebagaimana dimaksud pada ayat (1) huruf b merupakan pengelolaan personel organisasi dan pihak ketiga, termasuk peningkatan kompetensi, kesadaran Keamanan SPBE, dan proses perekrutan untuk memastikan kepatuhan terhadap kebijakan dan prosedur Keamanan SPBE.

(4) Keamanan fisik sebagaimana dimaksud pada ayat (1) huruf c merupakan perlindungan infrastruktur fisik dan aset organisasi dari risiko Keamanan SPBE yang meliputi akses tidak sah, pencurian, dan kerusakan.

(5) Keamanan teknologi sebagaimana dimaksud pada ayat (1) huruf d merupakan penerapan teknologi keamanan yang melindungi kerahasiaan, keutuhan, ketersedian, keaslian, dan kenirsangkalan data dan informasi.

Pasal 14

(1) Fungsionalitas dan kinerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf c meliputi pemeriksaan terhadap fungsionalitas:
a. kelengkapan fungsi dan kinerja Keamanan SPBE;
b. kebenaran fungsi dan kinerja Keamanan SPBE; dan
c. kelayakan fungsi dan kinerja Keamanan SPBE.

(2) Kelengkapan fungsi dan kinerja Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf a untuk memeriksa pemenuhan atas rangkaian fungsi dan kinerja terhadap semua tugas dan tujuan yang ditentukan.

(3) Kebenaran fungsi dan kinerja Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf b untuk memeriksa kesesuaian keluaran hasil sistem dengan tingkat presisi yang diperlukan.

(4) Kelayakan fungsi dan kinerja Keamanan SPBE sebagaimana dimaksud pada ayat (1) huruf c untuk memeriksa kepatutan fungsi dan kinerja sistem dalam pencapaian tugas dan tujuan tertentu.

Pasal 15

Aspek Keamanan SPBE lainnya sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf d meliputi:
a. penilaian pemenuhan ketentuan peraturan perundang-undangan;
b. penilaian kesesuaian dalam rangka sertifikasi atau terdapat perubahan yang telah disertifikasi; dan/atau
c. tindak lanjut atas adanya informasi dan/atau laporan publik atas gangguan terhadap Keamanan SPBE, yang tidak dalam rangka penindakan tindak pidana.

Pasal 16

(1) Selain kriteria Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1), pelaksanaan Audit Keamanan SPBE harus memperhatikan kebijakan mikro terkait Keamanan SPBE.
(2) Kebijakan mikro sebagaimana dimaksud pada ayat (1) merupakan kebijakan internal Instansi Pusat dan Pemerintah Daerah.

Bagian Kelima
Bukti Audit Keamanan SPBE

Pasal 17

(1) Bukti Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 2 huruf d harus memenuhi aspek:
    a. kecukupan; dan
    b. ketepatan.
(2) Kecukupan sebagaimana dimaksud pada ayat (1) huruf a merupakan ukuran kuantitas bukti Audit Keamanan SPBE yang dipengaruhi oleh penilaian auditor Keamanan SPBE atas risiko Audit Keamanan SPBE dan kualitas bukti Audit Keamanan SPBE.
(3) Ketepatan sebagaimana dimaksud pada ayat (1) huruf b merupakan ukuran kualitas bukti Audit Keamanan SPBE yaitu relevan, valid, dan andal untuk mendukung hasil Audit Keamanan SPBE.

Pasal 18

(1) Bukti Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 17 dapat diperoleh melalui:
    a. inspeksi;
    b. observasi;
    c. permintaan keterangan;
    d. konfirmasi; dan/atau
    e. prosedur analitis.
(2) Bukti Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) dapat berbentuk dokumen elektronik dan/atau fisik.

Bagian Keenam
Kesimpulan Audit Keamanan SPBE

Pasal 19

(1) Kesimpulan Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 2 huruf e dinyatakan secara jelas.
(2) Kesimpulan Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) diberikan pada setiap prosedur pelaksanaan Audit Keamanan SPBE mencakup prosedur evaluasi:
    a. desain kontrol Keamanan SPBE;
    b. implementasi kontrol Keamanan SPBE; dan
    c. efektivitas kontrol Keamanan SPBE.

(3) Kesimpulan Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) menghasilkan konklusi Audit Keamanan SPBE.
(4) Konklusi Audit Keamanan SPBE sebagaimana dimaksud pada ayat (3) terdiri atas:
    a. memadai;
    b. perlu peningkatan; atau
    c. tidak memadai.
(5) Pemberian konklusi Audit Keamanan SPBE sebagaimana dimaksud pada ayat (4) mengacu pada matriks konklusi Audit Keamanan SPBE
(6) Matriks konklusi Audit Keamanan SPBE sebagaimana dimaksud pada ayat (5) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 20

(1) Evaluasi desain kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf a merupakan prosedur yang dilakukan auditor Keamanan SPBE untuk memperoleh keyakinan yang memadai bahwa desain kontrol Keamanan SPBE telah sesuai dengan kriteria Audit Keamanan SPBE yang digunakan.
(2) Evaluasi desain kontrol Keamanan SPBE sebagaimana dimaksud pada ayat (1) menghasilkan kesimpulan yang terdiri atas:
    a. memadai;
    b. perlu peningkatan; atau
    c. tidak memadai.

Pasal 21

(1) Evaluasi implementasi kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf b merupakan prosedur yang dilakukan Auditor Keamanan SPBE untuk memperoleh keyakinan yang memadai bahwa implementasi kontrol telah sesuai dengan desain kontrol Keamanan SPBE.
(2) Evaluasi implementasi kontrol Keamanan SPBE sebagaimana dimaksud pada ayat (1) menghasilkan kesimpulan yang terdiri atas:
    a. sesuai dengan desain kontrol; atau
    b. tidak sesuai dengan desain kontrol.

Pasal 22

(1) Evaluasi efektivitas kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf c merupakan prosedur yang dilakukan auditor Keamanan SPBE untuk:
    a. memperoleh keyakinan yang memadai bahwa kontrol Keamanan SPBE yang berjalan telah mencapai tujuannya dengan efektif; atau
    b. mengidentifikasi risiko yang terjadi karena adanya kelemahan desain dan/atau implementasi kontrol Keamanan SPBE.

(2) Evaluasi efektivitas kontrol Keamanan SPBE sebagaimana dimaksud pada ayat (1) menghasilkan kesimpulan yang terdiri atas:
   a. efektif;
   b. perlu peningkatan; atau
   c. belum efektif.

BAB III
TATA CARA AUDIT KEAMANAN SPBE

Bagian Kesatu
Umum

Pasal 23
Audit Keamanan SPBE dilaksanakan melalui:
a. pelaksanaan Audit Keamanan SPBE;
b. pelaporan Audit Keamanan SPBE;
c. tindak lanjut Audit Keamanan SPBE;
d. pendaftaran pelaksana Audit Keamanan SPBE; dan
e. pengalokasian sumber daya.

Bagian Kedua
Pelaksanaan Audit Keamanan SPBE

Paragraf 1
Umum

Pasal 24
Pelaksanaan Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 23 huruf a terdiri atas:
a. Audit Keamanan SPBE internal;
b. Audit Keamanan SPBE oleh LATIK Terakreditasi yang terdaftar; dan
c. Audit Keamanan SPBE oleh LATIK pemerintah.

Paragraf 2
Audit Keamanan SPBE Internal

Pasal 25
(1) Audit Keamanan SPBE internal sebagaimana dimaksud dalam Pasal 24 huruf a dilaksanakan untuk kebutuhan internal Instansi Pusat atau Pemerintah Daerah.
(2) Audit Keamanan SPBE internal sebagaimana dimaksud pada ayat (1) dilaksanakan dengan tahapan:
   a. perencanaan;
   b. pelaksanaan;
   c. pelaporan; dan
   d. pemantauan tindak lanjut.
(3) Audit Keamanan SPBE internal sebagaimana dimaksud pada ayat (1) dilaksanakan secara periodik oleh auditor pada unit kerja Instansi Pusat atau Pemerintah Daerah yang melaksanakan tugas dan fungsi di bidang pengawasan intern.
(4) Unit kerja Instansi Pusat atau Pemerintah Daerah yang melaksanakan tugas dan fungsi di bidang pengawasan

intern sebagaimana dimaksud pada ayat (2) dapat melibatkan pegawai aparatur sipil negara dari unit kerja lain yang memiliki kompetensi:
a. Audit TIK; dan/atau
b. audit keamanan informasi.

(5) Kompetensi Audit sebagaimana dimaksud pada ayat (3) dibuktikan dengan sertifikat pelatihan Audit TIK dan/atau audit keamanan informasi.

(6) Pelatihan audit sebagaimana dimaksud pada ayat (4) diselenggarakan oleh Badan atau lembaga pelatihan lain yang mendapat pengakuan dari Badan.

Pasal 26

(1) Audit Keamanan SPBE internal sebagaimana dimaksud dalam Pasal 25 mengacu pada kebijakan Instansi Pusat atau Pemerintah Daerah dengan objek dan kriteria Audit Keamanan SPBE yang sesuai dengan yang diatur dalam Peraturan Badan ini.

(2) Audit Keamanan SPBE internal sebagaimana dimaksud pada ayat (1) dilaksanakan sebelum pelaksanaan Audit Keamanan SPBE oleh LATIK pemerintah atau LATIK Terakreditasi yang terdaftar.

(3) Audit Keamanan SPBE internal sebagaimana dimaksud pada ayat (2) tidak menghilangkan kewajiban Audit Keamanan SPBE oleh LATIK pemerintah atau LATIK Terakreditasi yang terdaftar.

Pasal 27

Audit Keamanan SPBE internal sebagaimana dimaksud dalam Pasal 26 dilaksanakan dengan prosedur:
a. pemahaman kontrol Keamanan SPBE;
b. evaluasi desain kontrol Keamanan SPBE;
c. evaluasi implementasi kontrol Keamanan SPBE; dan
d. evaluasi efektivitas kontrol Keamanan SPBE.

Pasal 28

Pemahaman kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 27 huruf a dilakukan melalui identifikasi informasi terdokumentasi untuk memperoleh pemahaman yang memadai tentang kontrol Keamanan SPBE terhadap lingkup Audit Keamanan SPBE.

Pasal 29

(1) Evaluasi desain kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 27 huruf b menghasilkan kesimpulan.

(2) Dalam hal kesimpulan sebagaimana dimaksud pada ayat (1) hasilnya memadai atau perlu peningkatan, tim auditor pada unit kerja Instansi Pusat atau Pemerintah Daerah yang melaksanakan tugas dan fungsi di bidang pengawasan intern melakukan:
a. prosedur evaluasi implementasi kontrol Keamanan SPBE dengan cakupan uji petik yang cukup; dan
b. evaluasi efektivitas kontrol Keamanan SPBE.

(3) Dalam hal kesimpulan sebagaimana dimaksud pada ayat (1) hasilnya tidak memadai, tim auditor pada unit kerja Instansi Pusat atau Pemerintah Daerah yang melaksanakan tugas dan fungsi di bidang pengawasan intern melakukan prosedur evaluasi efektivitas kontrol Keamanan SPBE.

Pasal 30

(1) Evaluasi implementasi kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 27 huruf c menghasilkan kesimpulan.
(2) Dalam hal kesimpulan sebagaimana dimaksud pada ayat (1) hasilnya sesuai dengan desain kontrol, tim auditor pada unit kerja Instansi Pusat atau Pemerintah Daerah yang melaksanakan tugas dan fungsi di bidang pengawasan intern melakukan prosedur evaluasi efektivitas kontrol Keamanan SPBE dengan cakupan uji petik yang cukup.
(3) Dalam hal kesimpulan sebagaimana dimaksud pada ayat (1) hasilnya tidak sesuai dengan desain kontrol Keamanan SPBE, tim auditor pada unit kerja Instansi Pusat atau Pemerintah Daerah yang melaksanakan tugas dan fungsi di bidang pengawasan intern melakukan:
    a. penambahan cakupan uji petik dalam evaluasi implementasi kontrol Keamanan SPBE; dan
    b. prosedur evaluasi efektivitas kontrol Keamanan SPBE dengan cakupan uji petik yang ekstensif.

Pasal 31

Evaluasi efektivitas kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 27 huruf d menghasilkan kesimpulan.

Pasal 32

(1) Kesimpulan sebagaimana dimaksud dalam Pasal 29 ayat (1), Pasal 30 ayat (1), dan Pasal 31 dapat digunakan untuk menentukan konklusi Audit Keamanan SPBE internal.
(2) Konklusi Audit Keamanan SPBE internal sebagaimana dimaksud pada ayat (1) mendapatkan hasil memadai jika:
    a. hasil evaluasi desain kontrol memadai, hasil evaluasi implementasi kontrol sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol efektif atau perlu peningkatan; atau
    b. hasil evaluasi desain kontrol perlu peningkatan, hasil evaluasi implementasi kontrol sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol efektif.
(3) Konklusi Audit Keamanan SPBE internal sebagaimana dimaksud pada ayat (1) mendapatkan hasil perlu peningkatan jika:
    a. hasil evaluasi desain kontrol memadai, hasil evaluasi implementasi kontrol sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol belum efektif;
    b. hasil evaluasi desain kontrol memadai, hasil evaluasi implementasi kontrol tidak sesuai dengan desain

kontrol, dan hasil evaluasi efektivitas kontrol efektif; atau

c. hasil evaluasi desain kontrol perlu peningkatan, hasil evaluasi implementasi kontrol sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol perlu peningkatan.

(4) Konklusi Audit Keamanan SPBE internal sebagaimana dimaksud pada ayat (1) mendapatkan hasil tidak memadai jika hasil kesimpulan tidak memenuhi ketentuan sebagaimana dimaksud pada ayat (2) dan ayat (3).

Pasal 33

(1) Audit Keamanan SPBE internal sebagaimana dimaksud dalam Pasal 25 harus dituangkan dalam Peta Rencana SPBE pada Instansi Pusat dan Pemerintah Daerah.

(2) Audit Keamanan SPBE internal sebagaimana dimaksud pada ayat (1) disusun dengan memperhatikan:
   a. Aplikasi SPBE dan/atau Infrastruktur SPBE yang dimiliki Instansi Pusat dan Pemerintah Daerah;
   b. risiko pada Aplikasi SPBE dan/atau Infrastruktur SPBE;
   c. kategori Sistem Elektronik;
   d. tingkat vitalitas Sistem Elektronik; dan/atau
   e. Audit Keamanan SPBE yang sudah dilaksanakan sebelumnya.

Paragraf 3
Audit Keamanan SPBE oleh LATIK Terakreditasi yang Terdaftar

Pasal 34

Audit Keamanan SPBE oleh LATIK Terakreditasi yang terdaftar sebagaimana dimaksud dalam Pasal 24 huruf b dilakukan dengan tahapan:
a. penunjukan;
b. penugasan;
c. perencanaan; dan
d. pelaksanaan.

Pasal 35

(1) Penunjukan sebagaimana dimaksud dalam Pasal 34 huruf a dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan mengenai pengadaan barang dan/atau jasa pemerintah.

(2) Dalam melakukan penunjukan sebagaimana dimaksud pada ayat (1), Instansi Pusat atau Pemerintah Daerah harus menyediakan dokumen mengenai:
   a. lingkup Audit Keamanan SPBE; dan
   b. ringkasan hasil Audit Keamanan SPBE internal dengan objek Audit Keamanan SPBE yang sama paling lama 2 (dua) tahun sebelumnya.

Pasal 36

(1) Penugasan sebagaimana dimaksud dalam Pasal 34 huruf b diberikan oleh pimpinan LATIK Terakreditasi yang terdaftar kepada tim auditor Keamanan SPBE.
(2) Tim auditor Keamanan SPBE sebagaimana dimaksud pada ayat (1) beranggotakan auditor Keamanan SPBE yang telah teregistrasi pada Badan.
(3) Tim auditor Keamanan SPBE sebagaimana dimaksud pada ayat (2) bertindak sebagai:
    a. pengendali mutu;
    b. pengendali teknis;
    c. ketua tim; dan
    d. anggota tim.
(4) Pengendali mutu sebagaimana dimaksud pada ayat (3) huruf a bertugas memastikan pelaksanaan Audit Keamanan SPBE telah sesuai dengan kebijakan dan prosedur Audit Keamanan SPBE yang dimiliki oleh LATIK Terakreditasi yang terdaftar.
(5) Pengendali teknis sebagaimana dimaksud pada ayat (3) huruf b bertugas memastikan pelaksanaan Audit Keamanan SPBE telah memadai secara teknis sesuai dengan lingkup Audit Keamanan SPBE.
(6) Ketua tim sebagaimana dimaksud pada ayat (3) huruf c bertugas memimpin pelaksanaan Audit Keamanan SPBE.
(7) Anggota tim sebagaimana dimaksud pada ayat (3) huruf d bertugas melaksanakan prosedur Audit Keamanan SPBE.

Pasal 37

(1) Penugasan sebagaimana dimaksud dalam Pasal 36 dilaksanakan berdasarkan surat tugas tim auditor Keamanan SPBE.
(2) Surat tugas tim auditor Keamanan SPBE sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. nama auditor Keamanan SPBE;
    b. jabatan dalam tim auditor Keamanan SPBE;
    c. nama Instansi Pusat atau Pemerintah Daerah yang diaudit; dan
    d. lingkup Audit Keamanan SPBE.
(3) Tim auditor Keamanan SPBE sebagaimana dimaksud pada ayat (1) harus memiliki kompetensi Audit Keamanan SPBE yang dapat dipenuhi secara kolektif.

Pasal 38

(1) Perencanaan sebagaimana dimaksud dalam Pasal 34 huruf c dilakukan oleh tim auditor Keamanan SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. lingkup Audit Keamanan SPBE;
    b. analisis risiko Keamanan SPBE;
    c. kriteria Audit Keamanan SPBE; dan
    d. rencana pengujian Audit Keamanan SPBE.
(3) Lingkup Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a merupakan hasil kesepakatan

dengan klien Audit Keamanan SPBE terkait objek, organisasi, lokasi geografis, dan periode Audit Keamanan SPBE.

(4) Analisis risiko keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b merupakan proses identifikasi dan evaluasi risiko Keamanan SPBE yang relevan dengan lingkup Audit Keamanan SPBE.

(5) Kriteria Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf c merupakan identifikasi dan pemetaan kriteria kontrol Keamanan SPBE yang sesuai dengan lingkup Audit Keamanan SPBE.

(6) Rencana pengujian Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf d berisikan rencana prosedur pengujian yang harus dilakukan Auditor Keamanan Informasi atas kontrol Keamanan SPBE termasuk alokasi waktu, personel, dan alat bantu Audit Keamanan SPBE.

Pasal 39

Pelaksanaan sebagaimana dimaksud dalam Pasal 34 huruf d terdiri atas prosedur:

a. pemahaman kontrol Keamanan SPBE;
b. evaluasi desain kontrol Keamanan SPBE;
c. evaluasi implementasi kontrol Keamanan SPBE; dan
d. evaluasi efektivitas kontrol Keamanan SPBE.

Pasal 40

Pemahaman kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 39 huruf a dilakukan melalui identifikasi informasi terdokumentasi untuk memperoleh pemahaman yang memadai tentang kontrol Keamanan SPBE terhadap lingkup Audit Keamanan SPBE.

Pasal 41

(1) Evaluasi desain kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 39 huruf b menghasilkan kesimpulan.

(2) Dalam hal kesimpulan sebagaimana dimaksud pada ayat (1) hasilnya memadai atau perlu peningkatan, tim auditor Keamanan SPBE melakukan:
   a. prosedur evaluasi implementasi kontrol Keamanan SPBE dengan cakupan uji petik yang cukup; dan
   b. evaluasi efektivitas kontrol Keamanan SPBE.

(3) Dalam hal kesimpulan sebagaimana dimaksud pada ayat (1) hasilnya tidak memadai, tim auditor Keamanan SPBE melakukan prosedur evaluasi efektivitas kontrol Keamanan SPBE.

Pasal 42

(1) Evaluasi implementasi kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 39 huruf c menghasilkan kesimpulan.

(2) Dalam hal kesimpulan sebagaimana dimaksud pada ayat (1) hasilnya sesuai dengan desain kontrol, tim auditor Keamanan SPBE melakukan prosedur evaluasi efektivitas

kontrol Keamanan SPBE dengan cakupan uji petik yang cukup.

(3) Dalam hal kesimpulan sebagaimana dimaksud pada ayat (1) hasilnya tidak sesuai dengan desain kontrol Keamanan SPBE, tim auditor Keamanan SPBE melakukan:
   a. penambahan cakupan uji petik dalam evaluasi implementasi kontrol Keamanan SPBE; dan
   b. prosedur evaluasi efektivitas kontrol Keamanan SPBE dengan cakupan uji petik yang ekstensif.

Pasal 43

Evaluasi efektivitas kontrol Keamanan SPBE sebagaimana dimaksud dalam Pasal 39 huruf d menghasilkan kesimpulan.

Pasal 44

(1) Kesimpulan sebagaimana dimaksud dalam Pasal 41 ayat (1), Pasal 42 ayat (1), dan Pasal 43 digunakan untuk menentukan konklusi Audit Keamanan SPBE.
(2) Konklusi Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) mendapatkan hasil memadai jika:
   a. hasil evaluasi desain kontrol memadai, hasil evaluasi implementasi kontrol sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol efektif atau perlu peningkatan; atau
   b. hasil evaluasi desain kontrol perlu peningkatan, hasil evaluasi implementasi kontrol sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol efektif.
(3) Konklusi Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) mendapatkan hasil perlu peningkatan jika:
   a. hasil evaluasi desain kontrol memadai, hasil evaluasi implementasi kontrol sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol belum efektif;
   b. hasil evaluasi desain kontrol memadai, hasil evaluasi implementasi kontrol tidak sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol efektif; atau
   c. hasil evaluasi desain kontrol perlu peningkatan, hasil evaluasi implementasi kontrol sesuai dengan desain kontrol, dan hasil evaluasi efektivitas kontrol perlu peningkatan.
(5) Konklusi Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) mendapatkan hasil tidak memadai jika hasil kesimpulan tidak memenuhi ketentuan sebagaimana dimaksud pada ayat (2) dan ayat (3).

Pasal 45

LATIK Terakreditasi yang terdaftar harus menerbitkan surat keterangan untuk setiap Audit Keamanan SPBE yang dilaksanakannya sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 46

Ketentuan mengenai pelaksanaan Audit Keamanan SPBE oleh LATIK Terakreditasi yang terdaftar sebagaimana dimaksud dalam Pasal 34 sampai dengan Pasal 45 berlaku secara mutatis mutandis terhadap pelaksanaan Audit Keamanan SPBE oleh LATIK pemerintah yang dilaksanakan terhadap Aplikasi Khusus dan/atau Infrastruktur Instansi Pusat dan Pemerintah Daerah jika LATIK Terakreditasi yang terdaftar belum ada.

Paragraf 4
Audit Keamanan SPBE oleh LATIK Pemerintah

Pasal 47

Audit Keamanan SPBE oleh LATIK pemerintah sebagaimana dimaksud dalam Pasal 24 huruf c dilakukan dengan tahapan:
a. penugasan;
b. perencanaan; dan
c. pelaksanaan.

Pasal 48

(1) Penugasan sebagaimana dimaksud dalam Pasal 47 huruf a diberikan kepada tim auditor Keamanan SPBE pada LATIK pemerintah.
(2) Tim auditor Keamanan SPBE sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Kepala Badan.
(3) Tim auditor Keamanan SPBE sebagaimana dimaksud pada ayat (1) paling sedikit terdiri atas:
    a. pengendali mutu;
    b. pengendali teknis;
    c. ketua tim; dan
    d. anggota tim.
(4) Pengendali mutu sebagaimana dimaksud pada ayat (3) huruf a bertugas memastikan pelaksanaan Audit Keamanan SPBE telah sesuai dengan kebijakan dan prosedur Audit Keamanan SPBE yang dimiliki oleh LATIK pemerintah.
(5) Pengendali teknis sebagaimana dimaksud pada ayat (3) memadai secara teknis sesuai dengan lingkup Audit Keamanan SPBE.
(6) Ketua tim sebagaimana dimaksud pada ayat (3) huruf b bertugas memimpin Audit Keamanan SPBE.
(7) Anggota tim sebagaimana dimaksud pada ayat (3) huruf c bertugas melaksanakan prosedur Audit Keamanan SPBE.

Pasal 49

(1) Penugasan sebagaimana dimaksud dalam Pasal 48 dilaksanakan berdasarkan keputusan Kepala Badan tentang tim auditor Keamanan SPBE.
(2) Keputusan Kepala Badan sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. nama auditor Keamanan SPBE;

b. jabatan dalam tim auditor Keamanan SPBE;
c. nama Instansi Pusat atau Pemerintah Daerah yang diaudit; dan
d. lingkup Audit Keamanan SPBE.

(3) Tim auditor Keamanan SPBE sebagaimana dimaksud pada ayat (1) harus memiliki kompetensi Audit Keamanan SPBE yang dapat dipenuhi secara kolektif.

Pasal 50

(1) Perencanaan sebagaimana dimaksud dalam Pasal 47 huruf b dilakukan oleh auditor Keamanan SPBE dengan menyusun perencanaan Audit Keamanan SPBE.
(2) Ketentuan mengenai perencanaan Audit Keamanan SPBE oleh LATIK Terakreditasi yang terdaftar sebagaimana dimaksud dalam Pasal 38 berlaku secara mutatis mutandis terhadap perencanaan Audit Keamanan SPBE yang dilaksanakan LATIK pemerintah.

Pasal 51

Ketentuan mengenai pelaksanaan Audit Keamanan SPBE oleh LATIK Terakreditasi yang terdaftar sebagaimana dimaksud dalam Pasal 39 sampai dengan Pasal 44 berlaku secara mutatis mutandis terhadap pelaksanaan Audit Keamanan SPBE yang dilaksanakan LATIK pemerintah.

Pasal 52

LATIK pemerintah harus menerbitkan surat keterangan untuk setiap Audit Keamanan SPBE yang dilaksanakannya sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 53

Ketentuan mengenai pelaksanaan Audit Keamanan SPBE oleh LATIK pemerintah dilaksanakan terhadap Aplikasi Umum dan/atau Infrastruktur SPBE Nasional sebagaimana dimaksud dalam Pasal 47 sampai dengan Pasal 52 berlaku secara mutatis mutandis terhadap pelaksanaan Audit Keamanan SPBE oleh Badan yang dilaksanakan terhadap Aplikasi Khusus dan Infrastruktur SPBE Instansi Pusat tertentu yang ditetapkan sebagai IIV.

Bagian Ketiga
Pelaporan Audit Keamanan SPBE

Pasal 54

(1) Pelaporan Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 23 huruf b dilakukan dengan cara:
a. ketua tim Auditor Keamanan SPBE menyusun rancangan laporan hasil Audit Keamanan SPBE dengan memastikan tujuan Audit Keamanan SPBE tercapai;
a. rancangan laporan hasil Audit Keamanan SPBE direviu oleh pengendali teknis dan pengendali mutu;

b. rancangan laporan hasil Audit Keamanan SPBE yang telah direviu disampaikan oleh ketua tim Auditor Keamanan SPBE kepada pimpinan LATIK cakupan Keamanan SPBE;
c. pimpinan LATIK cakupan Keamanan SPBE mengesahkan laporan hasil Audit Keamanan SPBE; dan
d. laporan hasil Audit Keamanan SPBE yang telah disahkan disampaikan oleh pimpinan LATIK cakupan Keamanan SPBE kepada pimpinan Instansi Pusat atau Pemerintah Daerah dan ditembuskan kepada unit kerja yang melaksanakan tugas dan fungsi di bidang pengawasan intern pada Instansi Pusat dan Pemerintah Daerah.

(2) Laporan hasil Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) dapat diberikan kepada pihak lain atas pertimbangan dari Instansi Pusat dan Pemerintah Daerah.

Bagian Keempat
Tindak Lanjut Audit Keamanan SPBE

Pasal 55

(1) Tindak lanjut Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 23 huruf c dilakukan oleh Instansi Pusat dan Pemerintah Daerah.
(2) Pemantauan atas tindak lanjut sebagaimana dimaksud pada ayat (1) dilakukan oleh unit kerja yang melaksanakan tugas dan fungsi di bidang pengawasan intern pada Instansi Pusat dan Pemerintah Daerah.
(3) Hasil pemantauan atas tindak lanjut Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) disampaikan kepada:
a. LATIK pemerintah, untuk Aplikasi Umum dan Infrastruktur SPBE Nasional; dan
b. menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika dan Kepala Badan, untuk Aplikasi Khusus dan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah ditembuskan kepada Badan.

Pasal 56

Penyampaian hasil pemantauan atas Audit Keamanan SPBE untuk Aplikasi Umum dan Infrastruktur SPBE Nasional sebagaimana dimaksud dalam Pasal 55 ayat (3) huruf a dilakukan setiap bulan April tahun berjalan.

Pasal 57

Penyampaian hasil pemantauan atas Audit Keamanan SPBE untuk Aplikasi Khusus dan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah sebagaimana dimaksud dalam Pasal 55 ayat (3) huruf b dilakukan secara elektronik sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima
Pendaftaran Pelaksana Audit Keamanan SPBE

Paragraf 1
Umum

Pasal 58

Pendaftaran pelaksana Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 23 huruf d terdiri atas:
a. pendaftaran LATIK Terakreditasi; dan
b. pendaftaran auditor Keamanan SPBE.

Paragraf 2
Pendaftaran LATIK Terakreditasi

Pasal 59

(1) Pendaftaran LATIK Terakreditasi sebagaimana dimaksud dalam Pasal 58 huruf a dilakukan oleh pimpinan LATIK dengan mengajukan permohonan pendaftaran kepada Kepala Badan.
(2) Permohonan pendaftaran sebagaimana dimaksud pada ayat (1) dengan menyampaikan:
    a. surat permohonan;
    b. salinan akta pendirian badan hukum;
    c. struktur organisasi;
    d. dokumen sistem kendali mutu audit;
    e. daftar auditor Keamanan SPBE yang berstatus sebagai pegawai tetap dan tidak tetap;
    f. bukti akreditasi terkait dari lembaga pemerintah nonstruktural yang bertugas dan bertanggung jawab di bidang akreditasi lembaga penilaian kesesuaian;
    g. surat izin usaha; dan
    h. surat keterangan domisili.
(3) Pendaftaran LATIK Terakreditasi sebagaimana dimaksud pada ayat (2) dilaksanakan melalui pelayanan perizinan berusaha terintegrasi secara elektronik sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 60

(1) Dalam hal permohonan pendaftaran sebagaimana dimaksud dalam Pasal 59 dinyatakan valid dan lengkap, Badan menerbitkan surat tanda register.
(2) Surat tanda register sebagaimana dimaksud pada ayat (1) diberikan paling lambat 15 (lima belas) hari kerja setelah permohonan dinyatakan sesuai dan lengkap.
(3) Surat tanda register sebagaimana dimaksud pada ayat (2) berlaku sesuai dengan masa berlaku akreditasi dari lembaga pemerintah nonstruktural yang bertugas dan bertanggung jawab di bidang Akreditasi lembaga penilaian kesesuaian.
(4) LATIK Terakreditasi yang telah mendapatkan surat tanda register sebagaimana dimaksud pada ayat (1) dinyatakan sebagai LATIK Terakreditasi yang terdaftar.

(5) Badan mempublikasikan daftar LATIK Terakreditasi yang terdaftar sebagaimana dimaksud pada ayat (4) melalui laman resmi Badan.

Pasal 61

(1) Masa berlaku surat tanda register dapat diperpanjang dengan mengajukan permohonan kepada Kepala Badan paling lambat 30 (tiga puluh) hari kalender sebelum habis masa berlaku surat tanda register.
(2) Permohonan sebagaimana dimaksud pada ayat (1) diajukan dengan menyampaikan:
    a. surat permohonan;
    b. sertifikat akreditasi dari lembaga pemerintah nonstruktural yang bertugas dan bertanggung jawab di bidang akreditasi lembaga penilaian kesesuaian; dan
    c. daftar auditor Keamanan SPBE yang menjadi anggota.

Pasal 62

(1) Surat tanda register tidak berlaku apabila:
    a. habis masa berlaku;
    b. LATIK Terakreditasi yang terdaftar melanggar ketentuan peraturan perundang-undangan; atau
    c. LATIK Terakreditasi yang terdaftar dinyatakan pailit sesuai dengan ketentuan peraturan perundang-undangan.
(2) LATIK Terakreditasi yang terdaftar dengan surat tanda register tidak berlaku sebagaimana dimaksud pada ayat (1) dihapus dari daftar LATIK Terakreditasi yang terdaftar.

Pasal 63

LATIK Terakreditasi yang terdaftar menyampaikan:
a. laporan secara periodik atas pelaksanaan Audit Keamanan SPBE setiap bulan April dan Oktober; dan
b. laporan perubahan daftar auditor Keamanan SPBE paling lambat 2 (dua) hari kerja setelah perubahan keanggotaan dilakukan;

kepada Kepala Badan.

Paragraf 3
Pendaftaran Auditor Keamanan SPBE

Pasal 64

(1) Pendaftaran auditor Keamanan SPBE sebagaimana dimaksud dalam Pasal 58 huruf b dilakukan oleh pimpinan LATIK dengan mengajukan permohonan pendaftaran kepada Kepala Badan.
(2) Permohonan pendaftaran sebagaimana dimaksud pada ayat (1) disampaikan secara elektronik.
(3) Permohonan pendaftaran sebagaimana dimaksud pada ayat (2) dilakukan dengan menyampaikan:
    a. surat permohonan;

b. salinan ijazah pendidikan strata satu atau sederajat;
c. salinan sertifikat kompetensi auditor Keamanan SPBE yang diterbitkan oleh Lembaga Sertifikasi Profesi ruang lingkup auditor Keamanan SPBE;
d. dokumen pengalaman di bidang keamanan informasi atau teknologi informasi yang dibuktikan dengan surat tugas, surat penempatan, surat keputusan, atau kontrak kerja;
e. pakta integritas; dan
f. salinan bukti keanggotaan organisasi profesi.

(4) Dalam hal sertifikat kompetensi auditor Keamanan SPBE sebagaimana dimaksud pada ayat (3) huruf c belum tersedia karena belum tersedianya penyelenggara sertifikasi kompetensi, sertifikat kompetensi auditor Keamanan SPBE digantikan dengan dokumen lainnya yang berlaku dan menyatakan keahlian.

(5) Dalam hal organisasi profesi sebagaimana dimaksud pada ayat (3) huruf f belum terbentuk, tidak perlu melampirkan salinan bukti keanggotaan organisasi profesi.

Pasal 65

(1) Dalam hal permohonan pendaftaran sebagaimana dimaksud dalam Pasal 64 dinyatakan valid dan lengkap, Badan menerbitkan surat tanda register.

(2) Surat tanda register sebagaimana dimaksud pada ayat (1) diterbitkan paling lambat 14 (empat belas) hari kerja setelah pendaftaran dinyatakan valid dan lengkap.

(3) Surat tanda register sebagaimana dimaksud pada ayat (2) berlaku sesuai dengan masa berlaku sertifikat kompetensi auditor Keamanan SPBE, paling lama 3 (tiga) tahun.

(4) Auditor Keamanan SPBE yang telah memperoleh surat tanda register sebagaimana dimaksud pada ayat (3) dimuat dalam daftar auditor Keamanan SPBE.

(5) Badan mempublikasikan daftar auditor Keamanan SPBE yang telah memperoleh surat tanda register sebagaimana dimaksud pada ayat (4) melalui laman resmi Badan.

Pasal 66

(1) Masa berlaku surat tanda register dapat diperpanjang dengan mengajukan permohonan kepada Kepala Badan paling lambat 30 (tiga puluh) hari kalender sebelum habis masa berlaku surat tanda register.

(2) Permohonan sebagaimana dimaksud pada ayat (1) diajukan dengan menyampaikan:
a. surat permohonan;
b. salinan sertifikat kompetensi auditor Keamanan SPBE terbaru yang diterbitkan oleh Lembaga Sertifikasi Profesi di bidang keamanan siber yang berkaitan dengan Audit Keamanan SPBE; dan
c. salinan bukti keanggotaan organisasi profesi.

(3) Dalam hal sertifikat kompetensi auditor Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b belum tersedia karena belum tersedianya penyelenggara sertifikasi kompetensi, sertifikat kompetensi auditor Keamanan SPBE digantikan dengan dokumen lainnya yang berlaku dan menyatakan keahlian.
(4) Dalam hal organisasi profesi sebagaimana dimaksud pada ayat (2) huruf c belum ada, tidak perlu melampirkan salinan bukti keanggotaan.

Pasal 67

(1) Surat tanda register dinyatakan tidak berlaku apabila:
a. habis masa berlaku;
b. auditor Keamanan SPBE meninggal dunia;
c. auditor Keamanan SPBE mengundurkan diri dari organisasi profesi;
d. auditor Keamanan SPBE dikeluarkan dari keanggotaan organisasi profesi karena pelanggaran kode etik profesi; atau
e. auditor Keamanan SPBE terbukti melanggar ketentuan peraturan perundang-undangan.
(2) Auditor Keamanan SPBE dengan surat tanda register tidak berlaku sebagaimana dimaksud pada ayat (1) dihapus dari daftar auditor Keamanan SPBE.
(3) Auditor Keamanan SPBE dengan surat tanda register habis masa berlaku sebagaimana dimaksud pada ayat (1) huruf a dapat mengajukan permohonan pendaftaran kembali sesuai dengan ketentuan dalam Pasal 64 melalui LATIK Terakreditasi yang terdaftar.

Bagian Kelima
Pengalokasian Sumber Daya

Pasal 68

(1) Pengalokasian sumber daya sebagaimana dimaksud dalam Pasal 23 huruf e dilakukan dengan mengalokasikan sumber daya Audit Keamanan SPBE dengan memadai.
(2) Dalam mengalokasi sumber daya Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1), Instansi Pusat, Pemerintah Daerah, dan LATIK cakupan Keamanan SPBE menentukan:
a. jumlah auditor Keamanan SPBE;
b. jumlah hari pelaksanaan Audit Keamanan SPBE; dan
c. alat bantu Audit Keamanan SPBE.

Pasal 69

(1) Jumlah Auditor Keamanan SPBE sebagaimana dimaksud dalam Pasal 68 ayat (2) huruf a paling sedikit berjumlah 2 (dua) orang dalam 1 (satu) penugasan dan dapat ditambah sesuai kebutuhan.
(2) Kebutuhan sebagaimana dimaksud pada ayat (1) ditentukan dengan mempertimbangkan:

a. kompetensi yang dibutuhkan sesuai lingkup Audit Keamanan SPBE; dan
b. kompleksitas teknologi dalam lingkup Audit Keamanan SPBE.

Pasal 70

(1) Jumlah hari pelaksanaan Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 68 ayat (2) huruf b mengacu pada matriks jumlah hari pelaksanaan Audit Keamanan SPBE.
(2) Jumlah hari pelaksanaan Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) berlaku untuk satu prosedur pelaksanaan Audit Keamanan SPBE.
(3) Jumlah hari pelaksanaan Audit Keamanan SPBE sebagaimana dimaksud pada ayat (2) ditentukan dengan mempertimbangkan:
    a. kompleksitas objek Audit Keamanan SPBE;
    b. kompleksitas teknologi objek Audit Keamanan SPBE; dan
    c. sebaran lokasi objek Audit Keamanan SPBE.
(4) Kompleksitas objek Audit Keamanan SPBE sebagaimana dimaksud pada ayat (3) huruf a paling sedikit mengacu pada matriks kompleksitas objek Audit Keamanan SPBE.
(5) Kompleksitas teknologi objek Audit Keamanan SPBE sebagaimana dimaksud pada ayat (3) huruf b paling sedikit mengacu pada matriks kompleksitas teknologi objek Audit Keamanan SPBE.
(6) Sebaran lokasi objek Audit Keamanan SPBE sebagaimana dimaksud pada ayat (3) huruf c dibedakan berdasarkan lokasi fisik yaitu:
    a. terpusat; dan
    b. tersebar.
(7) Matriks objek Audit Keamanan SPBE sebagaimana dimaksud pada ayat (3) sampai dengan ayat (6) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 71

(1) Alat bantu Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 68 ayat (2) huruf c merupakan perangkat teknologi yang digunakan auditor Keamanan SPBE dalam pelaksanaan pengujian kontrol keamanan.
(2) Dalam menentukan penggunaan alat bantu Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) LATIK cakupan Keamanan SPBE harus mempertimbangkan:
    a. kompleksitas teknologi dalam objek Audit Keamanan SPBE; dan
    b. keamanan alat bantu Audit Keamanan SPBE yang digunakan.

BAB IV
PENDANAAN AUDIT KEAMANAN SPBE

Pasal 72

(1) Instansi Pusat dan Pemerintah Daerah menyusun perencanaan dan penganggaran pelaksanaan Audit Keamanan SPBE sesuai dengan siklus perencanaan dan penganggaran.
(2) Besaran biaya Audit Keamanan SPBE dihitung dengan mempertimbangkan kompleksitas objek audit, sebaran lokasi, dan jumlah hari pelaksanaan audit.
(3) Pendanaan berasal dari:
    a. Anggaran Pendapatan dan Belanja Negara;
    b. anggaran pendapatan dan belanja daerah; dan/atau
    c. sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
KETENTUAN PENUTUP

Pasal 73

Peraturan Badan ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Badan ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 9 Oktober 2024

KEPALA BADAN SIBER DAN SANDI NEGARA,

Ditandatangani secara elektronik oleh:
KEPALA BADAN SIBER DAN SANDI NEGARA
Hinsa Siburian
Letnan Jenderal TNI (Purn)

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 9 Oktober 2024

Plt. DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

#KUMHAMPASTI
Ditandatangani secara elektronik oleh :

ASEP N. MULYANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2024 NOMOR 655

LAMPIRAN I
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 8 TAHUN 2024
TENTANG
STANDAR DAN TATA CARA PELAKSANAAN AUDIT KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

MATRIKS KONKLUSI AUDIT KEAMANAN SPBE

Hasil Evaluasi Desain Kontrol	Hasil Evaluasi Implementasi Kontrol	Hasil Evaluasi Efektivitas Kontrol	Konklusi Audit Keamanan SPBE
Memadai	Sesuai Dengan Desain Kontrol	Efektif	Memadai
		Perlu Peningkatan	Memadai
		Belum Efektif	Perlu Peningkatan
	Tidak Sesuai Dengan Desain Kontrol	Efektif	Perlu Peningkatan
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai
Perlu Peningkatan	Sesuai Dengan Desain Kontrol	Efektif	Memadai
		Perlu Peningkatan	Perlu Peningkatan
		Belum Efektif	Tidak Memadai
	Tidak Sesuai Dengan Desain Kontrol	Efektif	Tidak Memadai
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai
Tidak Memadai	-	Efektif	Tidak Memadai
		Perlu Peningkatan	Tidak Memadai
		Belum Efektif	Tidak Memadai

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

LAMPIRAN II
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 8 TAHUN 2024
TENTANG
STANDAR DAN TATA CARA PELAKSANAAN AUDIT KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

MATRIKS OBJEK KEAMANAN AUDIT KEAMANAN SPBE

A. MATRIKS JUMLAH HARI PELAKSANAAN AUDIT KEAMANAN SPBE

Kompleksitas Objek Audit	Kompleksitas Teknologi Objek Audit Keamanan SPBE	Sebaran Lokasi Objek Audit Keamanan SPBE	Jumlah Hari (paling singkat)*
Sederhana	Sederhana	Terpusat	2
		Tersebar	3
	Sedang	Terpusat	3
		Tersebar	4
	Kompleks	Terpusat	4
		Tersebar	5
Sedang	Sederhana	Terpusat	5
		Tersebar	6
	Sedang	Terpusat	6
		Tersebar	7
	Kompleks	Terpusat	7
		Tersebar	8
Kompleks	Sederhana	Terpusat	8
		Tersebar	9
	Sedang	Terpusat	9
		Tersebar	10
	Kompleks	Terpusat	10
		Tersebar	10

* untuk 1 tim auditor (paling sedikit dua orang) untuk satu prosedur pelaksanaan audit

B. MATRIKS KOMPLEKSITAS OBJEK AUDIT KEAMANAN SPBE

Indikator	Tingkat Kompleksitas Objek Audit		
	Sederhana	Sedang	Kompleks
Aplikasi SPBE	Aplikasi Khusus Instansi Pusat	Aplikasi Khusus Pemerintah Daerah	Aplikasi Umum SPBE Nasional
Pusat Data Nasional			Nasional
Jaringan Intra	Instansi Pusat	Pemerintah Daerah	Nasional
Sistem Penghubung Layanan	Instansi Pusat	Pemerintah Daerah	Nasional

C. MATRIKS KOMPLEKSITAS TEKNOLOGI OBJEK AUDIT KEAMANAN SPBE

Indikator	Tingkat Kompleksitas Teknologi		
	Sederhana	Sedang	Kompleks
UMUM			
Jumlah Personil TI	< 5 orang	6-10 orang	> 10 orang
Jumlah Pengguna	< 100 pengguna	100-1000 pengguna	> 1000 pengguna
Jenis Dampak Kegagalan	Operasional saja	Operasional dan Finansial	Operasional, Finansial, dan Legal
APLIKASI			
Sebaran peladen	Terpusat	Terdistribusi Dalam Negeri	Terdistribusi Dalam & Luar Negeri
Platform Teknologi	1 jenis	2-3 jenis	> 3 jenis
Waktu Pengembangan	< 3 bulan	3-12 bulan	> 12 bulan
Usia Sistem	< 1 tahun	1–3 tahun	> 3 tahun
Transaksi per hari	< 5000	5000 s.d. 50.000	> 50.000
Pola Pemrosesan	*Batch*	*Realtime*	*Hybrid*
Cakupan Proses Bisnis	< 30 %	30-60%	> 60%
INFRASTRUKTUR – PUSAT DATA NASIONAL			
Pengelolaan	Alih Daya, Sewa	Mandiri	Campuran
Strata SNI	Strata 1-2	Strata 3	Strata 4
Sertifikasi	Belum Ada	SNI 27001	SNI 27001 dan Standar Lain
INFRASTRUKTUR – JARINGAN INTRA			
Pengelolaan	Alih Daya, Sewa	Mandiri	Campuran
Cakupan Jaringan	*Local Area Network*, *Cluster Area Network*	*Metropolitan Area Network*, *Virtual Private Network*	*Wide Area Network*, Nasional
Media Jaringan	Kabel	Nirkabel	Kabel & Nirkabel
INFRASTRUKTUR – SISTEM PENGHUBUNG LAYANAN			
Cakupan Sistem	Intra Instansi Pusat atau Intra Pemerintah Daerah	Antar Instansi Pusat atau Antar Pemerintah Daerah	Nasional
Sifat Sistem	Tertutup	Semi Terbuka	Terbuka
Konten Sistem	Data	Aplikasi	Layanan
Sifat Informasi yang Dihubungkan	Terbuka	Terbatas	Tertutup

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN