LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH

SALINAN

KEPUTUSAN

KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH

REPUBLIK INDONESIA

NOMOR 207 TAHUN 2024

TENTANG

PEDOMAN PENYELENGGARAAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI ATAS SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH

KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH,

Menimbang :

a. bahwa untuk melaksanakan kegiatan audit teknologi informasi dan komunikasi sistem pemerintahan berbasis elektronik dalam rangka menjamin kualitas penyelenggaraan sistem pemerintahan berbasis elektronik, perlu menetapkan standar dan tata cara pelaksanaan audit teknologi informasi dan komunikasi sistem pemerintahan berbasis elektronik di lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a, perlu menetapkan Keputusan Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah tentang Pedoman Pelaksanaan Audit Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah;

Mengingat : 1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
2. Peraturan Menteri Komunikasi dan Informatika Nomor 16 Tahun 2022 tentang Kebijakan Umum Penyelenggaraan Audit Teknologi Informasi dan Komunikasi (Berita Negara Republik Indonesia Tahun 2022 Nomor 1374);
3. Peraturan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 2 Tahun 2023 tentang Organisasi dan Tata Kerja Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah (Berita Negara Republik Indonesia Tahun 2023 Nomor 112);
4. Keputusan Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 145 Tahun 2022 tentang Pedoman Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah;

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH TENTANG PEDOMAN PENYELENGGARAAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI ATAS SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH.

KESATU : Menetapkan Pedoman Penyelenggaraan Audit Teknologi Informasi dan Komunikasi atas Sistem Pemerintahan Berbasis Elektronik di Lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah yang selanjutnya disebut Pedoman Penyelenggaraan Audit TIK SPBE sebagaimana tercantum Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Pedoman Penyelenggaraan Audit TIK SPBE sebagaimana dimaksud pada diktum KESATU digunakan sebagai pedoman dalam melaksanakan Audit Infrastruktur, Audit Aplikasi dan Audit Keamanan pada Sistem Pemerintahan Berbasis Elektronik di Lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah.

KETIGA : Keputusan ini mulai berlaku pada tanggal ditetapkan dan apabila dikemudian hari terdapat kekeliruan dalam Keputusan ini, maka akan diadakan perbaikan sebagaimana mestinya.

Ditetapkan di Jakarta
Pada tanggal 14 Juni 2024
KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH,

ttd

HENDRAR PRIHADI

Salinan sesuai dengan aslinya
Kepala Biro Hukum, Organisasi dan
Sumber Daya Manusia LKPP,

Suharti

LAMPIRAN	:	KEPUTUSAN KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH TENTANG PEDOMAN PENYELENGGARAAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI ATAS SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH
NOMOR	:	207 TAHUN 2024
TANGGAL	:	14 Juni 2024

BAB I
PENDAHULUAN

Ketentuan Umum

1. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan dan penyampaian atau pemindahan informasi antar sarana/media.
2. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan TIK untuk memberikan layanan kepada Pengguna SPBE.
3. Proses Bisnis adalah sekumpulan kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi instansi pusat dan pemerintah daerah masing-masing.
4. 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.
5. 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.

6. Instansi Pusat adalah kementerian, lembaga pemerintah nonkementerian, kesekretariatan lembaga negara, kesekretariatan lembaga nonstruktural, dan lembaga pemerintah lainnya.
7. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
8. Audit Teknologi Informasi dan Komunikasi yang selanjutnya disebut Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset TIK dengan tujuan untuk menetapkan tingkat kesesuaian antara TIK dengan kriteria dan/atau standar yang telah ditetapkan.
9. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
10. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi Aplikasi SPBE dan yang memiliki nilai manfaat.
11. Arsitektur SPBE adalah kerangka dasar yang mendeskripsikan integrasi Proses Bisnis, data dan informasi, Infrastruktur SPBE, Aplikasi SPBE, dan keamanan SPBE untuk menghasilkan Layanan SPBE yang terintegrasi.
12. Peta Rencana SPBE adalah dokumen yang mendeskripsikan arah dan langkah penyiapan dan pelaksanaan SPBE yang terintegrasi.
13. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan atau menyebarkan informasi elektronik.
14. *Auditee* adalah unit organisasi yang menjadi obyek dari pelaksanaan Audit TIK.
15. Auditor TIK adalah orang yang memiliki kompetensi di bidang Audit TIK dan diberikan tugas untuk melakukan Audit TIK berdasarkan ketentuan peraturan perundang-undangan.
16. Pusat Data adalah fasilitas yang digunakan untuk penempatan Sistem Elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
17. Pusat Data Nasional adalah sekumpulan Pusat Data yang digunakan secara bagi pakai oleh Instansi Pusat dan Pemerintah Daerah, dan saling terhubung.

18. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
19. Jaringan Intra Pemerintah adalah jaringan interkoneksi tertutup yang menghubungkan antar Jaringan Intra Instansi Pusat dan Pemerintah Daerah.
20. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
21. Sistem Penghubung Layanan Pemerintah adalah perangkat terintegrasi yang terhubung dengan Sistem Penghubung Layanan Instansi Pusat dan Pemerintah Daerah untuk pertukaran Layanan SPBE antar Instansi Pusat dan/atau Pemerintah Daerah.
22. Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah yang selanjutnya disebut LKPP adalah lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden.

BAB II
PELAKSANAAN AUDIT TIK

A. Penjelasan Umum

1. Audit TIK pada LKPP merupakan Audit TIK yang dilaksanakan pada lingkup Instansi Pusat.
2. Audit TIK pada LKPP dilaksanakan terhadap:
   a. Infrastruktur SPBE;
   b. Aplikasi SPBE; dan
   c. Keamanan SPBE.
3. Audit TIK pada LKPP mencakup:
   a. Audit Infrastruktur SPBE;
   b. Audit Aplikasi SPBE;
   c. Audit Keamanan atas Infrastruktur SPBE dan/atau
   d. Audit Keamanan atas Aplikasi SPBE.
4. Audit TIK sebagaimana angka 1 harus dilaksanakan secara periodik, paling sedikit 1 (satu) kali dalam 2 (dua) tahun.
5. Audit TIK meliputi pemeriksaan hal pokok teknis pada:
   a. Penerapan tata kelola dan manajemen TIK;
   b. Fungsionalitas TIK;
   c. Kinerja TIK yang dihasilkan; dan
   d. Aspek TIK lainnya.
6. Audit TIK dilaksanakan berdasarkan arahan pimpinan atau permintaan dari unit organisasi yang memiliki fungsi pengelolaan TIK SPBE kepada pihak internal maupun eksternal sesuai dengan ruang lingkup audit dan kebutuhan LKPP.
7. Audit TIK Internal dilaksanakan oleh unit organisasi yang memiliki fungsi pengawasan internal di LKPP dan dapat dibantu oleh unit organisasi yang memiliki fungsi pengelolaan TIK SPBE.
8. Audit TIK Eksternal dilaksanakan oleh lembaga pelaksana Audit TIK pemerintah atau lembaga pelaksana Audit TIK terakreditasi dan terdaftar sesuai dengan ketentuan peraturan perundang-undangan.

B. Audit pada Penerapan Tata Kelola dan Manajemen TIK

1. Audit TIK terhadap tata kelola TIK meliputi pemeriksaan terhadap kerangka kerja pengaturan, pengarahan, dan pengendalian dalam penerapan SPBE secara terpadu atas unsur-unsur SPBE LKPP.
2. Unsur-unsur SPBE LKPP adalah sebagai berikut:
   a. Arsitektur SPBE;
   b. Peta Rencana SPBE;
   c. Rencana dan Anggaran SPBE;
   d. Proses Bisnis;
   e. Data dan Informasi;
   f. Infrastruktur SPBE;
   g. Aplikasi SPBE;
   h. Keamanan SPBE; dan
   i. Layanan SPBE.
3. Pemeriksaan atas kerangka kerja mencakup pemeriksaan atas aktivitas sebagai berikut:
   a. Evaluasi TIK;
   b. Pengarahan TIK; dan
   c. Pemantauan TIK.
4. Evaluasi TIK dilakukan dengan meninjau pemanfaatan TIK saat ini dan masa depan dengan memperhatikan kebutuhan LKPP.
5. Pengarahan TIK merupakan penetapan tanggung jawab serta pemberian arahan atas penyiapan dan pelaksanaan dari rencana dan kebijakan TIK serta mendorong suatu budaya tata kelola TIK yang baik.
6. Pemantauan TIK merupakan kegiatan memonitor kinerja TIK melalui sistem pengukuran yang tepat serta memastikan bahwa TIK sesuai dengan kebutuhan pemangku kepentingan.
7. Audit TIK terhadap manajemen TIK meliputi pemeriksaan terhadap tahapan sebagai berikut:
   a. Perencanaan TIK;
   b. Pengembangan TIK;
   c. Pengoperasian TIK; dan
   d. Pemantauan TIK.
8. Perencanaan TIK meliputi seluruh ketentuan peraturan internal, standar, dan prosedur serta proses yang terkait perencanaan strategis dan perencanaan taktis atas kegiatan dan anggaran yang terkait.

9. Pengembangan TIK meliputi seluruh ketentuan peraturan internal, standar, dan prosedur serta proses yang terkait dengan perancangan, pengadaan, pengembangan, pengujian, instalasi, migrasi, dan pelatihan TIK.
10. Pengoperasian TIK meliputi seluruh ketentuan peraturan perundang-undangan, ketentuan peraturan internal, standar, dan prosedur serta proses yang terkait dengan pengoperasian TIK.
11. Pemantauan TIK meliputi seluruh ketentuan peraturan internal, standar, dan prosedur serta proses yang terkait dengan pemantauan dan evaluasi TIK.
12. Audit TIK terhadap manajemen TIK meliputi pemeriksaan terhadap aktivitas sebagai berikut:
    a. Manajemen keamanan TIK;
    b. Manajemen risiko TIK;
    c. Manajemen aset TIK;
    d. Manajemen pengetahuan TIK;
    e. Manajemen sumber daya manusia TIK;
    f. Manajemen layanan TIK;
    g. Manajemen perubahan TIK; dan/atau
    h. Manajemen data TIK.
13. Manajemen keamanan TIK harus memperhatikan prinsip-prinsip:
    a. Kerahasiaan;
    b. Integritas;
    c. Ketersediaan;
    d. Keautentikan;
    e. Otorisasi; dan
    f. Kenirsangkalan TIK.

    Sesuai dengan ketentuan peraturan perundang-undangan.

C. Audit pada Fungsionalitas dan Kinerja TIK

1. Audit TIK terhadap fungsionalitas TIK merupakan pemeriksaan atas sejauh mana TIK dapat menyediakan fungsi yang memenuhi kebutuhan pada saat digunakan dalam kondisi yang sesuai spesifikasi, meliputi:
    a. Kelengkapan fungsi;
    b. Kebenaran fungsi; dan
    c. Kelayakan fungsi.

2. Audit TIK terhadap fungsionalitas TIK dan kinerja TIK yang dihasilkan mencakup:
   a. Aplikasi SPBE;
   b. Infrastruktur SPBE; dan
   c. Keamanan SPBE.
3. Aplikasi SPBE meliputi komponen perangkat lunak Sistem Elektronik yang digunakan untuk menjalankan fungsi, proses, dan mekanisme kerja SPBE.
4. Infrastruktur SPBE LKPP terdiri atas:
   a. Pusat Data Nasional;
   b. Pusat Data LKPP;
   c. *Public Cloud*;
   d. Jaringan Intra Pemerintah;
   e. Jaringan Intra LKPP;
   f. Sistem Penghubung Layanan Pemerintah
   g. Sistem Penghubung Layanan LKPP;
   h. Pusat Komputasi; dan
   i. Pusat Kendali.
5. Keamanan SPBE meliputi keamanan Aplikasi SPBE dan Infrastruktur SPBE.
6. Audit TIK terhadap kinerja TIK yang dihasilkan merupakan pemeriksaan atas sumber daya TIK yang digunakan pada kondisi yang sesuai spesifikasi, meliputi:
   a. Waktu;
   b. Utilisasi; dan
   c. Kapasitas.

D. Audit pada Aspek TIK Lainnya

1. Audit TIK terhadap aspek TIK lainnya meliputi:
   a. Audit kepatuhan TIK;
   b. Audit sertifikasi TIK; dan/atau
   c. Audit investigasi TIK.
2. Audit kepatuhan TIK merupakan Audit TIK untuk menilai pemenuhan ketentuan peraturan perundang-undangan.

3. Audit sertifikasi TIK merupakan Audit TIK untuk menilai kesesuaian dalam rangka sertifikasi atau terdapat perubahan TIK yang telah disertifikasi.
4. Audit investigasi TIK merupakan Audit TIK sebagai tindak lanjut atas adanya informasi dan/atau laporan publik atas gangguan terhadap TIK yang dilaksanakan tidak dalam rangka penindakan tindak pidana.

E. Pedoman Umum Audit TIK

1. Penyelenggaraan Audit TIK dilakukan paling sedikit dengan tahapan:
   a. Perencanaan audit;
   b. Pelaksanaan audit; dan
   c. Pelaporan audit.
2. Tahapan Penyelenggaraan audit TIK dilaksanakan sesuai dengan:
   a. Pedoman umum Audit TIK; dan
   b. Standar, tata cara, dan jangka waktu pelaksanaan Audit TIK.
3. Standar dan tata cara pelaksanaan Audit TIK terhadap Infrastruktur SPBE dan Aplikasi SPBE sesuai dengan Peraturan Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas pemerintah di bidang riset dan inovasi nasional untuk lingkup Audit Infrastruktur dan Aplikasi SPBE.
4. Standar dan tata cara pelaksanaan Audit TIK terhadap Keamanan SPBE sesuai dengan Peraturan Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas pemerintah di bidang keamanan siber untuk lingkup Audit Keamanan SPBE.
5. Unit organisasi yang memiliki fungsi pengawasan internal di LKPP selaku pelaksana Audit TIK harus menerbitkan laporan hasil Audit TIK untuk setiap Audit TIK yang telah dilaksanakan.
6. Auditor TIK harus mendokumentasikan seluruh informasi yang terkait dengan pelaksanaan prosedur audit dan berbagai bukti yang diperoleh di dalam kertas kerja Audit TIK, yang harus memenuhi ketentuan sebagai berikut:
   a. disusun menggunakan Bahasa Indonesia, dengan lengkap, jelas, terstruktur dan memiliki indeks, agar mudah untuk dipahami dan digunakan oleh pihak lain yang akan melakukan reviu atas kertas kerja audit tersebut; dan

b. mencantumkan identitas pihak yang melaksanakan setiap tahapan dan pengujian Audit TIK serta peranannya dan telah setujui oleh Ketua Tim dan Pengendali Teknis.

7. Auditor TIK harus mengelola dokumentasi atau kertas kerja Audit TIK atas suatu penugasan, yang antara lain mencakup catatan atau data mengenai:
   a. Perencanaan dan persiapan tujuan dan lingkup penugasan tersebut dan hasil telaahan atas dokumentasi audit sebelumnya atau yang terkait dengan penugasan tersebut;
   b. Hasil atau risalah rapat reviu pimpinan, rapat manajemen dan rapat lain yang terkait dengan penugasan tersebut;
   c. Pemahaman Auditor TIK tentang entitas atau kegiatan yang diaudit, dan lingkungan pengendalian intern serta sistem pemrosesan informasi yang terkait;
   d. Daftar program audit dan prosedur audit lainnya untuk memenuhi tujuan penugasan tersebut;
   e. Prosedur audit yang telah dilaksanakan dan bukti audit yang diperoleh dalam rangka mengevaluasi kelayakan dan kelemahan pengendalian TIK yang terkait dengan penugasan tersebut;
   f. Metode yang digunakan untuk menilai kelayakan pengendalian, adanya kelemahan atau kekurangan pengendalian, dan mengidentifikasi pengendalian pengganti *(compensating controls)*;
   g. Pembuat dan sumber dari dokumentasi audit beserta tanggal penyelesaiannya;
   h. Hak akses yang dimiliki dan/atau digunakan oleh Auditor TIK dalam pelaksanaan berbagai pengujian atas sumber daya TIK yang terkait;
   i. Hasil pengujian pengendalian, seperti pengujian atas kebijakan, prosedur dan pemisahan fungsi;
   j. Hasil pengujian terinci, seperti prosedur analitis, pengujian atas perhitungan, dan pengujian terinci lainnya;
   k. Berbagai hasil reviu atau telaahan hasil pelaksanaan supervisi audit;
   l. Berbagai temuan, kesimpulan dan rekomendasi audit yang terkait dengan penugasan tersebut;
   m. Tanggapan atau komentar pihak yang diaudit atas rekomendasi dari Auditor TIK;

n. Berbagai laporan yang diterbitkan sebagai hasil dari pelaksanaan penugasan tersebut; dan
o. Tanda terima dari pihak yang berhak untuk menerima laporan dan temuan audit.

8. Audit TIK harus disupervisi oleh pengendali teknis untuk memberikan jaminan yang memadai bahwa:
   a. Seluruh prosedur audit yang telah dialokasikan telah dilaksanakan dan didokumentasikan;
   b. Tidak terdapat prosedur audit yang tidak dilaksanakan oleh Tim Auditor TIK; dan
   c. Ketua Tim Auditor TIK telah melaksanakan reviu yang memadai atas seluruh dokumentasi pelaksanaan prosedur audit, kertas kerja audit serta bukti-bukti audit yang diperoleh.

BAB III
STANDAR PELAKSANAAN AUDIT TIK

Standar Pelaksanaan Audit TIK adalah batasan minimal bagi Regulator dan Auditor untuk membantu pelaksanaan audit serta prosedur yang harus dilaksanakan atau ditetapkan dalam rangka pencapaian tujuan audit. Standar pelaksanaan Audit TIK memiliki tujuan sebagai berikut:

1. Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit TIK;
2. Menyusun kerangka kerja dalam menyiapkan dan meningkatkan kompetensi Auditor di bidang Audit TIK;
3. Menyusun kerangka kerja dalam pemberian layanan jasa Audit TIK, guna memberikan nilai tambah kepada yang objek audit (*Auditee*) melalui perbaikan proses dan operasionalnya; dan
4. Menyusun dasar dalam melakukan evaluasi terhadap regulasi dan pelaksanaan Audit TIK guna mendorong rencana perbaikan.

A. Standar Umum

1. Standar umum memberikan prinsip dasar untuk mengatur Auditor TIK dalam melaksanakan tugasnya sehingga pelaksanaan pekerjaan Audit TIK hingga pelaporannya dapat terlaksana dengan baik dan efektif.
2. Integritas Auditor TIK diwujudkan melalui sikap independen, objektif, dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor TIK dituntut untuk menjalankan hal-hal sebagai berikut:
   a. Memiliki pengetahuan (*knowledge*), keterampilan (*skill*), sikap (*attitude*) dan pengalaman (*experience*) yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung jawabnya dalam pelaksanaan audit;
   b. Menggunakan keahlian profesionalnya dengan cermat dan seksama (*due professional care*) serta berhati-hati (*prudent*) dalam setiap penugasan;
   c. Senantiasa mengasah dan melatih kecermatan profesionalnya;
   d. Meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan; dan
   e. Mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan.

3. Tujuan, wewenang, dan tanggung jawab suatu aktivitas Audit TIK harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam pengawasan intern (*audit charter*), pedoman, surat tugas, atau dokumen-dokumen yang setara. Surat tugas atau piagam pengawasan intern (*audit charter*) wajib menjelaskan tujuan audit, ruang lingkup, kewenangan Tim Audit dan Etika yang harus dipatuhi oleh Tim Audit.
4. Inspektur LKPP memberikan tugas kepada Tim Audit dalam bentuk Surat Tugas.

B. Standar Pelaksanaan

1. Ketua Tim Audit (*Lead Auditor*) harus secara efektif mengelola aktivitas audit untuk menjamin agar tujuan Audit TIK tercapai. Ketua Tim Audit (*Lead Auditor*) harus melakukan hal-hal sebagai berikut:
   a. Menyusun dan menetapkan rencana audit (*audit plan*) guna menentukan prioritas-prioritas dalam kegiatan Audit TIK yang konsisten dengan tujuan audit sesuai dengan piagam pengawasan intern (*audit charter*);
   b. Menyampaikan rencana audit (*audit plan*) kepada *Auditee* untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumber daya;
   c. Mengelola sumber daya audit yang tepat, memadai, dan efektif untuk melaksanakan rencana audit yang telah disetujui;
   d. Melakukan koordinasi dengan pimpinan *Auditee* untuk menjamin bahwa pelaksanaan Audit TIK berjalan efektif dan efisien; dan
   e. Memberi laporan yang memadai kepada pimpinan *Auditee* mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.
2. Tujuan permintaan Audit TIK yang dapat diajukan tidak terbatas pada:
   a. Peningkatan kinerja birokrasi dan pelayanan publik;
   b. Penilaian kesesuaian dengan standar/prosedur/pedoman dan kesesuaian dengan rencana/kebutuhan/kondisi;
   c. Identifikasi status teknologi yang dimiliki, identifikasi kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
   d. Perencanaan pengembangan sistem/teknologi dan perencanaan perbaikan kelemahan; dan/atau

e. Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.

3. Pemeriksaan yang dilakukan terhadap *Auditee* mencakup:
   a. Penerapan tata kelola dan manajemen TIK SPBE;
   b. Fungsionalitas dan kinerja TIK SPBE; dan
   c. Tingkat kepatuhan terhadap regulasi.
4. Dalam hal merencanakan Audit TIK, Auditor TIK harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit TIK, termasuk tujuan, lingkup, waktu, dan alokasi sumber daya bagi pelaksanaan audit. Perencanaan tersebut yang dituangkan dalam rencana audit (*audit plan*) dengan mempertimbangkan berbagai hal, antara lain:
   a. Sistem pengendalian dan kepatuhan *Auditee* terhadap acuan atau *benchmark*;
   b. Penetapan tujuan Audit TIK;
   c. Penetapan kecukupan lingkup; dan
   d. Penggunaan metodologi yang tepat.
5. Dalam hal pelaksanaan Audit TIK, Auditor TIK harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai tujuan audit. Dalam melaksanakan audit tersebut, Auditor TIK harus:
   a. Memperoleh bukti-bukti audit yang cukup, handal, dan relevan untuk mendukung penilaian audit dan kesimpulan audit;
   b. Mendasarkan temuan dan kesimpulan audit pada analisis dan interpretasi yang memadai atas bukti-bukti audit;
   c. Menyiapkan, mengelola dan menyimpan data dan informasi yang diperoleh selama pelaksanaan audit; dan
   d. Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
6. Dalam hal telah terdapat hasil Audit TIK, Auditor TIK harus mengomunikasikan hasil pelaksanaan audit kepada pihak-pihak yang berkepentingan.
7. Komunikasi tersebut harus mencakup tujuan dan ruang lingkup pelaksanaan audit, selain kesimpulan yang terkait, rekomendasi dan rencana tindak lanjut. Jika penyampaian hasil audit terdapat kesalahan

atau penghilangan temuan yang signifikan, Ketua Tim Audit (*Lead Auditor*) harus mengomunikasikan kembali hasil audit yang telah diperbaiki kepada semua pihak.

8. Pelaksanaan kegiatan Audit TIK harus sesuai dengan kode etik dan standar audit.

C. Standar Pelaporan

1. Laporan hasil audit dibuat dalam bentuk dokumen laporan audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas.
2. Laporan hasil audit setidaknya harus memuat:
   a. Kondisi hasil audit (temuan hasil audit);
   b. Kriteria (standar/kebijakan yang diacu);
   c. Sebab;
   d. Akibat;
   e. Rekomendasi; dan
   f. Tanggapan *Auditee.*
3. Laporan audit harus mencantumkan batasan atau pengecualian yang berkaitan dengan pelaksanaan audit. Auditor TIK meminta tanggapan atau pendapat terhadap temuan, kesimpulan, dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh *Auditee* secara tertulis dari pimpinan *Auditee* yang bertanggung jawab.

D. Standar Tindak Lanjut

1. *Auditee* harus menindaklanjuti rekomendasi hasil Audit TIK dalam laporan hasil Audit TIK dan menyampaikan penyelesaian atas tindak lanjut rekomendasi hasil Audit TIK.
2. Pihak yang melaksanakan tindak lanjut hasil Audit TIK pada *Auditee* adalah Pejabat/pegawai yang disebutkan dalam rekomendasi hasil Audit TIK.
3. Inspektorat melakukan pemantauan tindak lanjut atas Rekomendasi Hasil Audit TIK melalui penilaian untuk memastikan kesesuaian tindak lanjut yang dilaksanakan oleh pihak yang dimaksud untuk melaksanakan tindak lanjut.

4. Jadwal pemantauan tindak lanjut hasil Audit TIK dilaksanakan secara periodik atau dalam waktu yang telah disepakati oleh Tim Audit dan *Auditee*.
5. Pemantauan tindak lanjut atas rekomendasi hasil audit dilakukan oleh Tim yang berbeda dengan Tim yang melaksanakan audit.

BAB IV
STANDAR TEKNIS DAN TATA CARA AUDIT TIK

A. STANDAR TEKNIS DAN TATA CARA AUDIT TIK

1. Pada prinsipnya standar teknis pelaksanaan Audit TIK dengan lingkup Audit TIK merujuk kepada standar, tata cara dan jangka waktu pelaksanaan yang diatur dalam ketentuan:
   a. Peraturan Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas pemerintah di bidang riset dan inovasi nasional untuk lingkup Audit Infrastruktur dan Aplikasi SPBE; dan
   b. Peraturan Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas pemerintah di bidang keamanan siber untuk lingkup Audit Keamanan SPBE.
2. Standar Teknis dan Tata Cara Audit TIK yang diuraikan terdiri dari:
   a. Standar Teknis dan Tata Cara Audit Infrastruktur SPBE;
   b. Standar Teknis Audit dan Tata Cara Audit Aplikasi SPBE; dan
   c. Standar Teknis dan Tata Cara Audit Keamanan Infrastruktur dan Aplikasi SPBE.
3. Standar Teknis dan Tata Cara Audit TIK akan dilakukan evaluasi secara berkala untuk menjamin efektivitas penggunaannya dengan memperhatikan peraturan perundang-undangan, standar audit yang berlaku serta dinamika perubahan pengawasan intern pemerintah.

B. STANDAR TEKNIS DAN TATA CARA AUDIT INFRASTRUKTUR SPBE

1. Ruang Lingkup Audit Infrastruktur SPBE
   a. Pelaksanaan Audit Infrastruktur SPBE dilaksanakan secara *online* menggunakan aplikasi *Audit Tools*, namun apabila aplikasi *Audit Tools* terkendala atau ruang lingkup audit tidak dapat diakomodir oleh aplikasi, maka pelaksanaan audit dapat menggunakan instrumen audit lain sesuai kebutuhan dengan memperhatikan ketentuan perundang-undangan.
   b. Lingkup Audit Infrastruktur SPBE diselenggarakan terhadap Infrastruktur SPBE yang digunakan oleh LKPP.
   c. Audit Infrastruktur SPBE di lingkungan LKPP dilakukan terhadap Aspek:
      1) Pusat Data;

2) Sistem Penghubung Layanan; dan
3) Jaringan Intra.

2. Standar Teknis Audit TIK Pusat Data
   a. Standar teknis Audit TIK Pusat Data di lingkungan LKPP bertujuan sebagai panduan dalam pelaksanaan Audit SPBE Pusat Data. Audit teknis terhadap Pusat Data yang mencakup fungsionalitas dan kinerja dengan lingkup yang terdiri atas:
      1) Perencanaan Pusat Data;
      2) Pengembangan Pusat Data;
      3) Pengoperasian Pusat Data; dan
      4) Pemeliharaan Pusat Data.
   b. Aktivitas audit terhadap perencanaan Pusat Data dilakukan untuk memperoleh keyakinan yang memadai bahwa:
      1) Penyelenggaraan Pusat Data telah sesuai dengan Arsitektur SPBE Nasional, Arsitektur SPBE Instansi Pusat, Peta Rencana SPBE Nasional, Peta Rencana SPBE Instansi Pusat;
      2) Perencanaan Pusat Data telah mencakup:
         a) Analisis kebutuhan;
         b) Pengelolaan lokasi;
         c) Bangunan;
         d) Penanganan kebakaran;
         e) Kelistrikan;
         f) Suhu;
         g) Pengkabelan;
         h) Pembagian ruangan;
         i) Sistem monitoring lingkungan;
         j) Persediaan bahan bakar;
         k) Sistem pendingin; dan
         l) Sistem jaringan data.
      3) Pengembangan yang dilakukan oleh Tim Internal Organisasi atau dengan menggunakan jasa pihak ketiga telah melalui pengujian implementasi, instalasi dan pengujian untuk mengetahui kesesuaian antara deskripsi dalam rancangan yang telah ditetapkan dengan pengembangan yang dilakukan;

4) Uji coba Pusat Data terhadap Pusat Data Nasional telah terdokumentasi dalam suatu rencana pengujian (*test plan*), rancangan pengujian (*test design*), prosedur pengujian (*test procedures*) dan laporan pengujian (*test report*);
5) Pusat Data dilengkapi dengan dokumentasi penggunaan Pusat Data, baik untuk operator maupun administrator;
6) Dokumentasi penggunaan Pusat Data telah mencakup:
   a) Organisasi;
   b) Tata kerja;
   c) Manajemen operasi;
   d) Pusat pemulihan bencana;
   e) Infrastruktur;
   f) Manajemen sumber daya manusia Pusat Data;
   g) Monitoring, pelaporan dan pengendalian; dan
   h) Manajemen layanan Pusat Data.
7) Pemeliharaan yang dilakukan telah didokumentasikan dalam suatu dokumen yang mencakup:
   a) Pemeliharaan;
   b) Manajemen konfigurasi perangkat; dan
   c) Pemantauan.

3. Standar Teknis Audit Jaringan Intra
   a. Standar teknis audit Jaringan Intra Pemerintah dimaksudkan sebagai panduan dalam pelaksanaan Audit Jaringan Intra Pemerintah di lingkungan LKPP.
   b. Aktivitas audit teknis Jaringan Intra Pemerintah dilakukan terhadap cakupan fungsionalitas dan kinerja.
   c. Lingkup panduan teknis audit Jaringan Intra Pemerintah terdiri atas:
      1) Perencanaan Jaringan Intra Pemerintah;
      2) Pengembangan Jaringan Intra Pemerintah;
      3) Pengoperasian Jaringan Intra Pemerintah; dan
      4) Pemeliharaan Jaringan Intra Pemerintah.
   d. Aktivitas audit terhadap Jaringan Intra Pemerintah dilakukan untuk memperoleh keyakinan yang memadai bahwa:

1) Perencanaan telah mengacu kepada Arsitektur SPBE Nasional, Arsitektur SPBE LKPP, Peta Rencana SPBE Nasional dan Peta Rencana SPBE LKPP;
2) Perencanaan Jaringan Intra Pemerintah telah disusun berdasarkan persyaratan Jaringan Intra Pemerintah dengan mempertimbangkan kebutuhan dan Infrastruktur SPBE Nasional yang mencakup:
   a) Kebutuhan bisnis;
   b) Kebutuhan jaringan dan rancangan jaringan.
3) Jaringan Intra Pemerintah dapat dikembangkan oleh Tim Internal LKPP atau menggunakan jasa pihak ketiga dengan mengacu kepada deskripsi dalam rancangan;
4) Konfigurasi jaringan SPBE dapat disesuaikan dan dilengkapi dengan dokumentasi yang memadai;
5) Uji coba terhadap Jaringan Intra Pemerintah harus terdokumentasi dalam:
   a) Rencana pengujian (*test plan*);
   b) Rancangan pengujian (*test design*);
   c) Prosedur pengujian (*test procedures*); dan
   d) Laporan pengujian (*test report*).
6) Jaringan Intra Pemerintah telah dilengkapi dengan dokumentasi penggunaan Jaringan Intra Pemerintah baik untuk Operator maupun Administrator yang mencakup:
   a) Penggunaan perangkat Jaringan Intra Pemerintah antara lain cara instalasi, akses terhadap perangkat, operasi terhadap perangkat;
   b) Prosedur dan tutorial; dan
   c) Gangguan dan penanganannya.
7) Pemeliharaan terhadap Jaringan Intra Pemerintah telah didokumentasikan dalam suatu dokumen yang mencakup pemeliharaan jaringan dan manajemen konfigurasi jaringan.

4. Standar Teknis Sistem Penghubung Layanan Pemerintah
   a. Standar teknis audit Sistem Penghubung Layanan Pemerintah dimaksudkan sebagai panduan dalam pelaksanaan Audit Infrastruktur SPBE.

b. Audit teknis Sistem Penghubung Layanan Pemerintah mencakup fungsionalitas dan kinerja.
c. Lingkup panduan teknis Audit Sistem Penghubung Layanan Pemerintah terdiri atas:
    1) Perencanaan Sistem Penghubung Layanan Pemerintah;
    2) Pengembangan Sistem Penghubung Layanan Pemerintah;
    3) Pengoperasian Sistem Penghubung Layanan Pemerintah; dan
    4) Pemeliharaan Sistem Penghubung Layanan Pemerintah.
d. Aktivitas audit terhadap perencanaan Sistem Penghubung Layanan Pemerintah dilakukan untuk memperoleh keyakinan yang memadai bahwa:
    1) Sistem Penghubung Layanan Pemerintah direncanakan dengan mengacu kepada Arsitektur SPBE nasional, Arsitektur SPBE LKPP, Peta Rencana SPBE Nasional dan Peta Rencana SPBE LKPP.
    2) Perencanaan Sistem Penghubung Layanan Pemerintah telah mencakup:
        a) Prinsip;
        b) Kebijakan; dan
        c) Organisasi.
    3) Sistem Penghubung Layanan Pemerintah dapat dikembangkan oleh Tim Internal LKPP atau menggunakan jasa pihak ketiga dengan mengacu kepada deskripsi dalam rancangan.
    4) Pengembangan Sistem Penghubung Layanan Pemerintah mencakup implementasi, pengujian dan instalasi.
    5) Uji coba terhadap Sistem Penghubung Layanan Pemerintah harus terdokumentasi dalam:
        a) Rencana pengujian (*test plan*);
        b) Rancangan pengujian (*test design*);
        c) Prosedur pengujian (*test procedures*); dan
        d) Laporan pengujian (*test report*).
    6) Sistem Penghubung Layanan Pemerintah dilengkapi dengan dokumentasi penggunaan Sistem Penghubung Layanan Pemerintah baik untuk Operator maupun Administrator yang mencakup penyelenggaraan dan mekanisme kerja.

7) Pemeliharaan terhadap Jaringan Intra Pemerintah didokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:
   a) Lingkup pemeliharaan;
   b) Alokasi sumber daya; dan
   c) Pencatatan kinerja.

5. Pengujian Terhadap Aspek Penerapan Infrastruktur SPBE
   a. Audit Infrastruktur SPBE dilaksanakan melalui serangkaian pengujian pada aspek penerapan Infrastruktur SPBE yang meliputi:
      1) Aspek tata kelola Infrastruktur SPBE;
      2) Aspek manajemen Infrastruktur SPBE;
      3) Aspek fungsionalitas dan kinerja Infrastruktur SPBE; dan
      4) Aspek lain SPBE.
   b. Dalam aspek penerapan tata kelola Infrastruktur SPBE, dilakukan pengujian terhadap aktivitas pengendalian yang mencakup:
      1) Evaluasi tata kelola;
      2) Pengarahan tata kelola; dan
      3) Pemantauan tata kelola.
   c. Dalam aspek penerapan manajemen infrastruktur, dilakukan pengujian terhadap aktivitas pengendalian pada setiap tahapan yang terdiri dari:
      1) Tahap perencanaan TIK, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
         a) Aktivitas pengendalian terhadap manajemen risiko;
         b) Aktivitas pengendalian terhadap manajemen sumber daya manusia;
         c) Aktivitas pengendalian terhadap manajemen data; dan
         d) Aktivitas pengendalian terhadap manajemen perencanaan layanan.
      2) Tahap pengembangan TIK, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
         a) Aktivitas pengendalian terhadap manajemen pengetahuan;
         b) Aktivitas pengendalian terhadap manajemen perubahan;
         c) Aktivitas pengendalian terhadap manajemen aset; dan

d) Aktivitas pengendalian terhadap manajemen pengembangan layanan.

3) Tahap pengoperasian TIK, berupa pengujian terhadap aktivitas pengendalian yang mencakup aktivitas pengendalian terhadap manajemen operasional layanan.

4) Tahap pemantauan TIK, berupa pengujian terhadap aktivitas pengendalian yang mencakup aktivitas pengendalian terhadap manajemen sistem pengendalian internal.

d. Dalam aspek penerapan fungsionalitas dan kinerja infrastruktur, dilakukan pengujian pada:

1) Jaringan Intra, pada setiap tahapan yang terdiri dari:

a) Tahap perencanaan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:

(1) Aktivitas pengendalian atas kebutuhan bisnis (*business requirement*);

(2) Aktivitas pengendalian atas kebutuhan jaringan (*network requirement*); dan

(3) Aktivitas pengendalian atas rancangan jaringan (*network design*).

b) Tahap pengembangan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:

(1) Aktivitas pengendalian atas implementasi jaringan (*network implementation*);

(2) Aktivitas pengendalian atas instalasi (*installation*); dan

(3) Aktivitas pengendalian atas pengujian (*testing*).

c) Tahap pengoperasian, berupa pengujian terhadap aktivitas pengendalian yang mencakup utilisasi/kinerja jaringan (*network utilization/performance*).

d) Tahap Pemantauan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:

(1) Aktivitas pengendalian terhadap pemeliharaan jaringan (*network maintenance*);

(2) Aktivitas pengendalian terhadap manajemen konfigurasi jaringan (*network configuration management*);

(3) Aktivitas pengendalian terhadap pengujian (*testing*).

2) Sistem Penghubung Layanan pada setiap tahapan yang terdiri dari:
   a) Tahap perencanaan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
      (1) Aktivitas pengendalian atas prinsip;
      (2) Aktivitas pengendalian atas kebijakan;
      (3) Aktivitas pengendalian atas organisasi;
      (4) Aktivitas pengendalian atas teknis; dan
      (5) Tahap pengembangan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
         (a) Aktivitas pengendalian atas implementasi Sistem Penghubung Layanan;
         (b) Aktivitas pengendalian terhadap instalasi (*installation*);
         (c) Aktivitas pengendalian atas pengujian (*testing*).
   b) Tahap pengoperasian, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
      (1) Aktivitas pengendalian atas penyelenggaraan Sistem Penghubung Layanan;
      (2) Aktivitas pengendalian atas dokumen mekanisme kerja.
   c) Tahap pemantauan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
      (1) Aktivitas pengendalian atas pemeliharaan Sistem Penghubung Layanan;
      (2) Aktivitas pengendalian atas manajemen konfigurasi jaringan (*network configuration management*);
      (3) Aktivitas Pengendalian atas Pengujian (*Testing*).

e. Dalam penerapan aspek lain Infrastruktur SPBE dilakukan pengujian terhadap:
   1) Aspek lain Jaringan Intra SPBE pada setiap tahapan yang terdiri dari:
      a) Tahap kepatuhan, berupa pengujian atas aktivitas pengendalian yang mencakup kepatuhan berkaitan dengan Aplikasi SPBE;
      b) Tahap sertifikasi, berupa pengujian atas aktivitas pengendalian yang mencakup kelaikan Jaringan Intra SPBE.

2) Aspek lain Sistem Penghubung Layanan SPBE pada setiap tahapan yang terdiri dari:
   a) Tahap kepatuhan, berupa pengujian atas aktivitas pengendalian yang mencakup:
      (1) Aktivitas pengendalian atas kepatuhan berkaitan dengan Aplikasi SPBE;
      (2) Aktivitas pengendalian atas standar.
   b) Tahap sertifikasi, berupa pengujian atas aktivitas pengendalian yang mencakup kelaikan Sistem Penghubung Layanan.

6. Kesimpulan Lingkup Audit Infrastruktur SPBE
   a. Kriteria, penilaian dan metode dalam penarikan kesimpulan hasil audit Infrastruktur SPBE mengacu pada ketentuan yang diatur oleh Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas pemerintah di bidang riset dan inovasi nasional;
   b. Kesimpulan Audit Infrastruktur SPBE diperoleh dengan memperhatikan:
      1) Hasil evaluasi desain kontrol penyelenggaraan Infrastruktur SPBE dibandingkan dengan standar yang digunakan sebagai kriteria audit;
      2) Hasil evaluasi implementasi kontrol penyelenggaraan Infrastruktur SPBE dibandingkan dengan desain kontrol Infrastruktur SPBE;
      3) Hasil evaluasi efektivitas kontrol Infrastruktur SPBE dibandingkan dengan tujuan kontrol Infrastruktur SPBE; dan
      4) Standar yang berlaku dan ketentuan perundang-undangan.

7. Tata Cara Audit Infrastruktur
   a. Pelaksanaan Audit Infrastruktur SPBE dilaksanakan secara daring menggunakan aplikasi audit *tools* yang dimiliki oleh Lembaga Pemerintah Nonkementerian yang menyelenggarakan tugas pemerintah di bidang riset dan inovasi nasional, maupun melalui peraturan yang berlaku.

b. Tata Cara Pelaksanaan Audit Infrastruktur SPBE dilakukan oleh Tim Audit Infrastruktur SPBE berdasarkan permintaan Unit Organisasi di lingkungan LKPP atau penugasan dari Inspektur.
c. Audit Infrastruktur SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar dilaksanakan dalam 3 (tiga) tahapan yaitu:
   1) Tahap perencanaan (*pre-audit*);
   2) Tahap pelaksanaan lapangan (*onsite audit*); dan
   3) Tahap analisa data dan pelaporan (*post audit*).
d. 3 (tiga) tahap pelaksanaan audit tersebut di atas meliputi aktivitas sebagai berikut:
   1) Penyiapan Tim Audit;
   2) *Quick assessment*;
   3) Penyiapan rencana audit;
   4) Penyepakatan rencana audit;
   5) Penyiapan tata cara audit;
   6) Penetapan parameter acuan;
   7) Pertemuan pembukaan;
   8) Pelaksanaan lapangan;
   9) Analisa data;
   10) Pengelolaan data;
   11) Penyusunan laporan;
   12) *Proof-read* laporan;
   13) Penyerahan laporan;
   14) Pertemuan penutupan; dan
   15) Evaluasi aktivitas.
e. Aktivitas yang dilaksanakan dalam setiap tahapan audit dilakukan untuk memperoleh keyakinan yang memadai bahwa:
   1) *Quick Assessment* dilakukan untuk mengenali obyek audit dengan mengidentifikasi: *current issue*, lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, Proses Bisnis dari organisasi atau bagian yang diaudit.
   2) Tim Audit Infrastruktur SPBE telah merencanakan tindakan audit yang dicantumkan dalam rencana audit (*audit plan*), dengan mendefinisikan hal-hal berikut:
      a) Tujuan audit;
      b) Lingkup;

c) Pendekatan;
d) Kriteria;
e) Parameter;
f) Acuan;
g) Metode pengumpulan data;
h) Penentuan objek;
i) Data primer dan sekunder;
j) Metode analisa;
k) *Deliverable*; dan
l) Perkiraan jadwal pelaksanaan.

3) Tim Audit dan *Auditee* menyepakati rencana audit sebelum tahap pelaksanaan audit.
4) Dalam pelaksanaan kegiatan audit, Tim Audit Infrastruktur SPBE berkewajiban untuk:
   a) Menyusun tata cara audit yang berisi detail instrumen audit, antara lain:
      (1) Daftar data, pertanyaan dan pengujian;
      (2) Formulir untuk mendokumentasikan data, jawaban, hasil observasi dan hasil pengujian;
      (3) Menetapkan parameter acuan untuk setiap kriteria diperlukan untuk memberikan suatu acuan pembanding;
      (4) Melakukan pertemuan pembukaan dengan *Auditee*;
      (5) Melaksanakan audit lapangan, melalui:
         (a) Penelaahan dokumen;
         (b) Wawancara;
         (c) Observasi lapangan;
         (d) Pengujian; dan
         (e) Verifikasi bukti;
   b) Melakukan analisis bukti;
   c) Mengelola data; dan
   d) Melakukan pertemuan penutupan dengan *Auditee*.
5) Data status penyelenggaraan SPBE diinventaris secara objektif berdasarkan fakta yang ada pada *Auditee*.
6) Deskripsi data dan informasi yang dikumpulkan merujuk pada kriteria penilaian sebagaimana ditentukan dalam peraturan yang diatur oleh Lembaga Pemerintah Non Kementerian yang

menyelenggarakan tugas pemerintah di bidang riset dan inovasi nasional.

7) Temuan Audit Infrastruktur SPBE merupakan keadaan dimana fakta status aset teknologi SPBE *Auditee* tidak sesuai dengan persyaratan Infrastruktur SPBE.
8) Pengurangan dan penambahan lingkup data, dapat dilakukan sepanjang relevan dengan objek dan rencana penggunaan hasil audit.
9) Kegiatan audit yang sedang berjalan telah dilakukan monitoring untuk mengidentifikasi *progress* pelaksanaan audit.
10) Evaluasi secara menyeluruh dilakukan setelah aktivitas audit selesai yang bertujuan untuk mengetahui kelebihan dan kekurangan aktivitas audit yang telah dilakukan dalam rangka meningkatkan kualitas pelaksanaan audit berikutnya.
11) Inspektur dapat menetapkan kebijakan tindak lanjut atas hasil evaluasi dari Tim Audit.

f. Pelaporan hasil Audit Infrastruktur SPBE disusun sesuai ketentuan tata naskah yang berlaku, dengan memperhatikan hal-hal sebagai berikut:
   1) Laporan audit disampaikan oleh Tim Audit secara berjenjang kepada Inspektur.
   2) Laporan hasil audit mencakup:
      a) Kondisi yang memerlukan perhatian pimpinan Unit Organisasi selaku *Auditee;*
      b) Risiko atau potensi risiko yang diidentifikasi;
      c) Kriteria dan/atau acuan metode pengumpulan data yang digunakan sesuai dengan lingkup Audit Infrastruktur SPBE;
      d) Hasil analisis, temuan, dan/atau kesimpulan audit;
      e) rekomendasi tindakan perbaikan yang dapat dilakukan oleh Unit Organisasi sebagai *Auditee*; dan
      f) Rencana tindak lanjut Unit Organisasi selaku *Auditee*.
   3) Kondisi yang memerlukan perhatian pimpinan Unit Organisasi selaku *Auditee* harus mencakup:
      a) Kelemahan dalam perencanaan aktivitas pengendalian dibandingan dengan kriteria pengendalian Infrastruktur SPBE yang digunakan; dan

b) Ketidaksesuaian antara implementasi Infrastruktur SPBE dengan perencanaan aktivitas pengendalian Infrastruktur SPBE.

4) Risiko atau potensi risiko yang diidentifikasi terdiri atas:
   a) Kelemahan perencanaan dan/atau implementasi aktivitas pengendalian Infrastruktur SPBE; dan
   b) Hasil pelaksanaan pengujian aktivitas pengendalian Infrastruktur SPBE.
5) Rekomendasi tindakan perbaikan yang dapat dilakukan oleh Auditee dilakukan untuk meningkatkan:
   a) Kecukupan aktivitas pengendalian Infrastruktur SPBE;
   b) Kesesuaian implementasi aktivitas pengendalian Infrastruktur SPBE; dan
   c) Efektivitas aktivitas pengendalian Infrastruktur SPBE.
6) *Draft* laporan direviu oleh Pengendali Teknis dan/atau Pengendali Mutu untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit.
7) Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh *Auditee* secara tertulis dari Pimpinan Unit Organisasi *Auditee*.
8) Laporan audit ditandatangani oleh Inspektur dan disampaikan kepada A*uditee*.

C. STANDAR TEKNIS DAN TATA CARA AUDIT APLIKASI SPBE

1. Ruang Lingkup Audit Aplikasi SPBE

a. Lingkup Audit Aplikasi SPBE diselenggarakan terhadap aset Aplikasi SPBE yang dimiliki oleh LKPP.
b. Audit Aplikasi SPBE di Lingkungan LKPP dilakukan terhadap aspek Aplikasi SPBE.

2. Standar Teknis Audit Aplikasi SPBE

a. Standar teknis Audit Aplikasi SPBE di lingkungan LKPP bertujuan sebagai acuan dalam menetapkan lingkup area audit aplikasi, kriteria audit dan penilaian status teknologi Aplikasi SPBE.
b. Audit teknis terhadap Aplikasi SPBE mencakup:

1) Tata kelola;
2) Manajemen;
3) Fungsionalitas dan Kinerja; dan
4) Aspek Lain.

c. Aktivitas audit terhadap Aplikasi SPBE dilakukan untuk memperoleh keyakinan yang memadai bahwa:
   1) Perencanaan aplikasi disusun dalam suatu dokumen menggunakan basis spesifikasi yang mencakup unsur:
      a) Kemampuan aplikasi; dan
      b) Persyaratan Proses Bisnis unit organisasi selaku *Auditee*.
   2) Kemampuan aplikasi telah mengacu kepada:
      a) Arsitektur SPBE secara berjenjang; dan
      b) Persyaratan bisnis organisasi.
   3) Arsitektur SPBE terdiri atas Arsitektur SPBE Nasional dan Arsitektur SPBE Instansi Pusat.
   4) Persyaratan Proses Bisnis *Auditee* dirumuskan dengan mempertimbangkan kebutuhan, peluang dan Proses Bisnis yang diterjemahkan ke dalam persyaratan aplikasi yang mencakup kebutuhan fungsi, antarmuka, data, kinerja dan batasan rancangan.
   5) Rancangan aplikasi disusun berdasarkan persyaratan aplikasi serta memperhatikan kesesuaiannya terhadap ketentuan perundang-undangan dan integrasi data, yang disertai dengan penjelasan yang didokumentasikan sebagai dokumen deskripsi rancangan aplikasi.
   6) Aplikasi SPBE dikembangkan oleh Tim Internal *Auditee* dan/atau pihak ketiga dengan mengacu kepada dokumen deskripsi rancangan aplikasi. Kode sumber (*source code*) aplikasi harus dilengkapi dengan dokumentasi yang memadai;
   7) Kode sumber (*source code*) aplikasi menggunakan *open source*, dapat dikustomisasi dan dilengkapi dengan dokumentasi yang memadai;
   8) Pengembangan Aplikasi SPBE harus disertai dengan uji coba fungsionalitasnya;
   9) Pembangunan aplikasi harus didokumentasikan dalam dokumen prosedur pembangunan aplikasi (*system build procedures*) yang

dilengkapi dengan panduan instalasi aplikasi untuk menerapkan aplikasi di lingkungan sistem yang ada;

10) Aplikasi yang dikembangkan mengacu pada ketentuan perundangan yang berlaku;
11) Pengembangan aplikasi harus dilengkapi dengan dokumentasi penggunaan aplikasi dan tanggung jawab data Pengguna;
12) Penggunaan aplikasi mencakup Pengguna dengan klasifikasi *End-Users* dan *Administrator*;
13) Dokumentasi penggunaan aplikasi mencakup:
    a) Penggunaan aplikasi secara umum, antara lain: cara instalasi, akses terhadap aplikasi, operasi terhadap data;
    b) Tutorial;
    c) Dokumen teknis; dan
    d) Pesan kesalahan dan penanganannya (*troubleshooting*).
14) Kinerja pengoperasian aplikasi dapat dievaluasi dari fungsi komponen perangkat lunak Sistem Elektronik yang digunakan untuk menjalankan SPBE.
15) Kinerja Sistem Elektronik untuk mendukung fungsi *Auditee* dikelompokkan ke dalam 3 klasifikasi, yaitu:
    a) Mampu mendukung semua fungsi Proses Bisnis *Auditee*;
    b) Mampu mendukung Sebagian fungsi Proses Bisnis *Auditee*; dan
    c) Belum mampu mendukung fungsi Proses Bisnis *Auditee*.
16) Pemeliharaan terhadap aplikasi di dokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:
    a) Lingkup pemeliharaan;
    b) Alokasi sumber daya;
    c) Pencatatan kinerja; dan
    d) Urutan/rangkaian proses pemeliharaan.
17) Perubahan terhadap aplikasi di dokumentasikan dalam suatu dokumen *software configuration management* yang mencakup:
    a) Lingkup konfigurasi;
    b) Aktivitas dan manajemen konfigurasi;
    c) Sumber daya konfigurasi; dan
    d) Penjadwalan manajemen konfigurasi.

18) Kriteria penilaian Audit Aplikasi SPBE dan kriteria penilaian Audit Aplikasi SPBE, merujuk kepada ketentuan yang diatur oleh Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas pemerintah di bidang riset dan inovasi nasional.

3. Pengujian Terhadap Aspek Penerapan Aplikasi SPBE

a. Audit Aplikasi SPBE dilaksanakan melalui serangkaian pengujian pada aspek penerapan Aplikasi SPBE yang meliputi:
   1) Aspek tata kelola Aplikasi SPBE;
   2) Aspek manajemen Aplikasi SPBE;
   3) Aspek fungsionalitas dan kinerja Aplikasi SPBE; dan
   4) Aspek lain Aplikasi SPBE.

b. Dalam aspek penerapan tata kelola Aplikasi SPBE, dilakukan pengujian terhadap aktivitas pengendalian yang mencakup:
   1) Evaluasi tata kelola;
   2) Pengarahan tata kelola; dan
   3) Pemantauan tata kelola.

c. Dalam aspek penerapan manajemen aplikasi, dilakukan pengujian terhadap aktivitas pengendalian pada setiap tahapan yang terdiri dari:
   1) Tahap perencanaan TIK, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
      a) Aktivitas pengendalian terhadap manajemen risiko;
      b) Aktivitas pengendalian terhadap manajemen sumber daya manusia;
      c) Aktivitas pengendalian terhadap manajemen data; dan
      d) Aktivitas pengendalian terhadap manajemen perencanaan layanan.
   2) Tahap pengembangan TIK, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
      a) Aktivitas pengendalian terhadap manajemen pengetahuan;
      b) Aktivitas pengendalian terhadap manajemen perubahan;
      c) Aktivitas pengendalian terhadap manajemen aset; dan
      d) Aktivitas pengendalian terhadap manajemen pengembangan layanan.

3) Tahap pengoperasian TIK, berupa pengujian terhadap aktivitas pengendalian yang mencakup aktivitas pengendalian terhadap manajemen operasional layanan.
4) Tahap pemantauan TIK, berupa pengujian terhadap aktivitas pengendalian yang mencakup aktivitas pengendalian terhadap manajemen sistem pengendalian internal.

d. Dalam aspek penerapan fungsionalitas dan kinerja aplikasi, dilakukan pengujian pada:
1) Aplikasi, pada setiap tahapan yang terdiri dari:
a) Tahap perencanaan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
(1) Aktivitas pengendalian atas persyaratan layanan (*business requirement*);
(2) Aktivitas pengendalian atas kebutuhan perangkat lunak (*software requirement*); dan
(3) Aktivitas pengendalian atas rancangan perangkat lunak (*software design*).
b) Tahap pengembangan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
(1) Aktivitas pengendalian atas implementasi perangkat lunak (*software implementation*);
(2) Aktivitas pengendalian atas pengujian (*testing*); dan
(3) Aktivitas pengendalian atas instalasi (*installation*);
c) Tahap pengoperasian, berupa pengujian terhadap aktivitas pengendalian yang mencakup penggunaan perangkat lunak (*software usage*).
d) Tahap pemeliharaan, berupa pengujian terhadap aktivitas pengendalian yang mencakup:
(1) Aktivitas pengendalian terhadap pemeliharaan perangkat lunak (*software maintenance*);
(2) Aktivitas pengendalian terhadap manajemen konfigurasi perangkat lunak (*software configuration management*); dan
(3) Aktivitas pengendalian terhadap pengujian (*testing*).

4. Kesimpulan Lingkup Audit Aplikasi SPBE

a. Kriteria, penilaian dan metode dalam penarikan kesimpulan hasil Audit Aplikasi SPBE mengacu pada ketentuan yang diatur oleh Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas pemerintah di bidang riset dan inovasi nasional;

b. Kesimpulan Audit Aplikasi SPBE diperoleh dengan memperhatikan:
   1) Hasil evaluasi desain kontrol Aplikasi SPBE dibandingkan dengan standar yang digunakan sebagai kriteria audit;
   2) Hasil evaluasi implementasi kontrol Aplikasi SPBE dibandingkan dengan desain kontrol Aplikasi SPBE;
   3) Hasil evaluasi efektivitas kontrol Aplikasi SPBE dibandingkan dengan tujuan kontrol Aplikasi SPBE; dan
   4) Standar yang berlaku dan ketentuan perundang-undangan.

5. Tata Cara Audit Aplikasi SPBE

a. Pelaksanaan Audit Aplikasi SPBE dilaksanakan secara *online* menggunakan aplikasi *audit tools*, namun apabila aplikasi *audit tools* terkendala dapat menggunakan instrumen audit lain sesuai kebutuhan dengan memperhatikan ketentuan perundang-undangan yang berlaku.

b. Tata cara pelaksanaan Audit Aplikasi SPBE dilakukan oleh Tim Audit Aplikasi SPBE berdasarkan permintaan Unit Organisasi di lingkungan LKPP atau penugasan dari Inspektur.

c. Audit Aplikasi SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar dilaksanakan dalam 3 (tiga) tahapan yaitu:
   1) Tahap perencanaan (*pre-audit*);
   2) Tahap pelaksanaan lapangan (*onsite audit*); dan
   3) Tahap analisa data dan pelaporan (*post audit*).

d. 3 (tiga) tahap pelaksanaan audit tersebut di atas meliputi aktivitas sebagai berikut:
   1) Penyiapan Tim Audit;
   2) *Quick assessment*;
   3) Penyiapan rencana audit;
   4) Penyepakatan rencana audit;
   5) Penyiapan tata cara audit;
   6) Penetapan parameter acuan;

7) Pertemuan pembukaan;
8) Pelaksanaan lapangan;
9) Analisa data;
10) Pengelolaan data;
11) Penyusunan laporan;
12) *Proof-read* laporan;
13) Penyerahan laporan;
14) Pertemuan penutupan; dan
15) Evaluasi aktivitas.

e. Aktivitas yang dilaksanakan dalam setiap tahapan audit dilakukan untuk memperoleh keyakinan yang memadai bahwa:
1) *Quick assessment* dilakukan untuk mengenali obyek audit dengan mengidentifikasi: *current issue*, lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, Proses Bisnis dari organisasi, atau bagian yang diaudit;
2) Tim Audit TIK telah merencanakan tindakan audit yang dicantumkan dalam rencana audit (*audit plan*), dengan mendefinisikan hal-hal berikut:
a) Tujuan audit;
b) Lingkup;
c) Pendekatan;
d) Kriteria;
e) Parameter;
f) Acuan;
g) Metode pengumpulan data;
h) Penentuan objek;
i) Data primer dan sekunder;
j) Metode analisa;
k) *Deliverable*; dan
l) Perkiraan jadwal pelaksanaan.
3) Tim Audit dan *Auditee* menyepakati rencana audit sebelum tahap pelaksanaan audit.
4) Dalam pelaksanaan kegiatan audit, Tim Audit Aplikasi SPBE berkewajiban untuk:
a) Menyusun tata cara audit yang berisi detail instrumen audit, antara lain:

(1) Daftar data, pertanyaan dan pengujian;
(2) Formulir untuk mendokumentasikan data, jawaban, hasil observasi dan hasil pengujian;
(3) Menetapkan parameter acuan untuk setiap kriteria diperlukan untuk memberikan suatu acuan pembanding;
(4) Melakukan pertemuan pembukaan dengan *Auditee*;
(5) Melaksanakan audit lapangan, melalui:
(a) Penelaahan dokumen;
(b) Wawancara;
(c) Observasi lapangan;
(d) Pengujian; dan
(e) Verifikasi bukti;

b) Melakukan analisis bukti;
c) Mengelola data; dan
d) Melakukan pertemuan penutupan dengan *Auditee*.

5) Data penyelenggaraan SPBE diinventaris secara objektif berdasarkan fakta yang ada pada *Auditee*.
6) Deskripsi data dan informasi yang dikumpulkan merujuk pada kriteria penilaian sebagaimana ditentukan dalam peraturan yang diatur oleh Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas Pemerintah di bidang riset dan inovasi nasional.
7) Pengurangan dan penambahan lingkup data, dapat dilakukan sepanjang relevan dengan objek dan rencana penggunaan hasil audit.
8) Temuan Audit Infrastruktur SPBE merupakan keadaan dimana fakta status aset teknologi SPBE *Auditee* tidak sesuai dengan persyaratan Infrastruktur SPBE.
9) Kegiatan audit yang sedang berjalan telah dilakukan monitoring untuk mengidentifikasi *progress* pelaksanaan audit.
10) Evaluasi secara menyeluruh dilakukan setelah aktivitas audit selesai yang bertujuan untuk mengetahui kelebihan dan kekurangan aktivitas audit yang telah dilakukan dalam rangka meningkatkan kualitas pelaksanaan audit berikutnya.
11) Inspektur dapat menetapkan kebijakan tindak lanjut atas hasil evaluasi dari Tim Audit.

f. Pelaporan hasil Audit Aplikasi SPBE disusun sesuai ketentuan tata naskah yang berlaku, dengan memperhatikan hal-hal sebagai berikut:
   1) Laporan audit disampaikan oleh Tim Audit secara berjenjang kepada Inspektur;
   2) Laporan hasil audit mencakup:
      a) Kondisi yang memerlukan perhatian pimpinan Unit Organisasi selaku *Auditee;*
      b) Risiko atau potensi risiko yang diidentifikasi;
      c) Kriteria dan/atau acuan metode pengumpulan data yang digunakan sesuai dengan lingkup Audit Aplikasi SPBE;
      d) Hasil analisis, temuan, dan/atau kesimpulan audit;
      e) rekomendasi tindakan perbaikan yang dapat dilakukan oleh Unit Organisasi sebagai *Auditee*; dan
      f) Rencana tindak lanjut Unit Organisasi selaku *Auditee*.
   3) Kondisi yang memerlukan perhatian pimpinan Unit Organisasi selaku Auditee harus mencakup:
      a) Kelemahan dalam perencanaan aktivitas pengendalian dibandingan dengan kriteria pengendalian Aplikasi SPBE yang digunakan; dan
      b) Ketidaksesuaian antara implementasi Aplikasi SPBE dengan perencanaan aktivitas pengendalian Aplikasi SPBE.
   4) Risiko atau potensi risiko yang diidentifikasi terdiri atas:
      a) Kelemahan perencanaan dan/atau implementasi aktivitas pengendalian Aplikasi SPBE; dan
      b) Hasil pelaksanaan pengujian aktivitas pengendalian Aplikasi SPBE.
   5) Rekomendasi tindakan perbaikan yang dapat dilakukan oleh Auditee dilakukan untuk meningkatkan:
      a) Kecukupan aktivitas pengendalian Aplikasi SPBE;
      b) Kesesuaian implementasi aktivitas pengendalian Aplikasi SPBE; dan
      c) Efektivitas aktivitas pengendalian Aplikasi SPBE.
   6) Draf laporan direviu oleh Pengendali Teknis dan/atau Pengendali Mutu untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit;

7) Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh *Auditee* secara tertulis dari Pimpinan *Auditee*; dan
8) Laporan Audit ditandatangani oleh Ketua Tim, Pengendali Teknis dan Inspektur serta disampaikan kepada *Auditee*.

D. STANDAR TEKNIS DAN TATA CARA AUDIT KEAMANAN SPBE

1. Ruang Lingkup Standar Teknis Audit Keamanan SPBE

a. Lingkup Audit Keamanan SPBE di lingkungan LKPP terdiri atas:
   1) Audit keamanan infrastruktur;
   2) Audit keamanan aplikasi; dan
   3) Kompleksitas Audit Keamanan SPBE di lingkungan LKPP.
b. Cakupan Audit Keamanan SPBE di lingkungan LKPP terdiri atas:
   1) Audit keamanan Infrastruktur SPBE; dan
   2) Audit keamanan Aplikasi SPBE.
c. Aspek Teknis Audit Keamanan SPBE di lingkungan LKPP terdiri atas:
   1) Penerapan tata kelola keamanan;
   2) Penerapan manajemen keamanan;
   3) Fungsionalitas keamanan; dan
   4) Kinerja keamanan.
d. Infrastruktur SPBE LKPP terdiri atas:
   1) Sistem Penghubung Layanan; dan
   2) Jaringan Intra.

2. Standar Teknis Audit Keamanan SPBE

a. Standar teknis Audit Keamanan SPBE di lingkungan LKPP bertujuan sebagai panduan dalam pelaksanaan Audit Keamanan SPBE dengan lingkup Audit Jaringan Intra dan Sistem Penghubung Layanan.
b. Tahapan Audit Keamanan Jaringan Intra Pemerintah terdiri atas:
   1) Perencanaan Jaringan Intra Pemerintah;
   2) Pengembangan Jaringan Intra Pemerintah;
   3) Pengoperasian Jaringan Intra Pemerintah; dan
   4) Pemeliharaan Jaringan Intra Pemerintah.
c. Tahapan Audit Keamanan Sistem Penghubung Layanan Pemerintah terdiri atas:
   1) Perencanaan Sistem Penghubung Layanan Pemerintah;

2) Pengembangan Sistem Penghubung Layanan Pemerintah;
3) Pengoperasian Sistem Penghubung Layanan Pemerintah; dan
4) Pemeliharaan Sistem Penghubung Layanan Pemerintah.

d. Aktivitas audit dalam lingkup Keamanan SPBE dilakukan untuk memperoleh keyakinan yang memadai bahwa:
   1) Aspek Teknis Audit Keamanan Aplikasi SPBE dan Infrastruktur SPBE LKPP terdiri atas:
      a) Penerapan tata kelola keamanan;
      b) Penerapan manajemen keamanan;
      c) Fungsionalitas keamanan; dan
      d) Kinerja keamanan.
   2) Tahapan pada aspek teknis tata kelola keamanan adalah pengujian atas kontrol keamanan dalam:
      a) Pengevaluasian;
      b) Pengarahan;
      c) Pemantauan; dan
      d) Komunikasi.
   3) Tahapan pada aspek teknis manajemen keamanan telah mencakup pengujian atas kontrol keamanan dalam:
      a) Perencanaan;
      b) Pelaksanaan;
      c) Evaluasi; dan
      d) Peningkatan.
   4) Tahapan pada aspek teknis fungsionalitas keamanan adalah pengujian terhadap kontrol keamanan dalam:
      a) Kelengkapan fungsi;
      b) Kebeneran fungsi; dan
      c) Kelayakan fungsi.
   5) Tahapan pada aspek teknis kinerja keamanan adalah pengujian terhadap kontrol keamanan dalam:
      a) Waktu;
      b) Utilisasi; dan
      c) Kapasitas.
   6) Pelaksanaan Audit Keamanan SPBE telah menggunakan instrumen penilaian.
   7) Audit Keamanan SPBE telah mengacu pada:

a) Standar Nasional Indonesia; dan
b) Peraturan perundang-undangan terkait Keamanan Informasi.

3. Pengujian Terhadap Aspek Penerapan Keamanan SPBE

a. Audit atas Keamanan SPBE, dilaksanakan melalui serangkaian pengujian atas aktivitas pengendalian pada Aspek Penerapan Keamanan SPBE yang meliputi:
   1) Aspek tata kelola keamanan;
   2) Aspek sistem manajemen keamanan;
   3) Aspek pengendalian keamanan; dan
   4) Aspek fungsionalitas dan kinerja keamanan.
b. Dalam aspek tata kelola Keamanan SPBE, dilakukan pengujian terhadap aktivitas pengendalian yang mencakup:
   1) Pengevaluasian;
   2) Pengarahan;
   3) Pemantauan; dan
   4) Komunikasi.
c. Dalam aspek penerapan sistem manajemen keamanan, dilakukan pengujian terhadap aktivitas pengendalian yang mencakup:
   1) Perencanaan;
   2) Pelaksanaan;
   3) Evaluasi; dan
   4) Peningkatan.
d. Dalam aspek pengendalian keamanan, dilakukan pengujian berdasarkan analisis terhadap tingkat risiko keamanan atas aktivitas pengendalian yang mencakup:
   1) Teknologi;
   2) Personil;
   3) Fisik; dan
   4) Organisasi.
e. Dalam aspek fungsionalitas dan kinerja, dilakukan pengujian terhadap aktivitas pengendalian yang mencakup:
   1) Perencanaan;
   2) Pengembangan;
   3) Pengoperasian; dan
   4) Pemantauan.

f. Aktivitas pengujian dalam pelaksanaan Audit Keamanan SPBE juga dilakukan terhadap:
   1) Kesesuaian aspek pengendalian keamanan dengan Standar Nasional Indonesia; dan
   2) Kesesuaian aspek pengendalian keamanan dengan peraturan perundang-undangan terkait Keamanan Informasi.

4. Kesimpulan Lingkup Audit Keamanan SPBE

a. Audit Keamanan SPBE menghasilkan kesimpulan:
   1) Memadai;
   2) Perlu peningkatan; atau
   3) Tidak memadai.

b. Kesimpulan Audit Keamanan SPBE diperoleh dengan memperhatikan:
   1) Hasil evaluasi desain kontrol Keamanan SPBE dibandingkan dengan standar yang digunakan sebagai kriteria audit;
   2) Hasil evaluasi implementasi kontrol Keamanan SPBE dibandingkan dengan desain kontrol Keamanan SPBE; dan
   3) Hasil evaluasi efektivitas kontrol Keamanan SPBE dibandingkan dengan tujuan kontrol Keamanan SPBE.

c. Penarikan kesimpulan Audit Keamanan SPBE mengacu pada matriks kesimpulan Audit Keamanan SPBE yang diatur dalam ketentuan yang dibuat oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

5. Tata Cara Audit Keamanan SPBE

a. Tata cara Audit Keamanan SPBE mengacu pada tata cara Audit Keamanan SPBE yang diatur dalam mekanisme yang disusun oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

b. Tata cara pelaksanaan Audit Keamanan SPBE pada tahapan pelaksanaan terdiri dari:
   1) Permintaan, dengan uraian berupa:
      a) Permintaan Audit Keamanan SPBE dilakukan dengan mengirimkan surat permintaan Audit Keamanan SPBE kepada

Inspektorat dari Unit Organisasi atau Penugasan dari Inspektur.

b) Surat permintaan Audit Keamanan SPBE ditandatangani oleh Pimpinan Unit Organisasi.

c) Surat permintaan Audit Keamanan SPBE mencakup:

(1) Informasi umum identitas Unit Organisasi;

(2) Informasi umum lingkup Audit Keamanan SPBE;

(3) Lokasi pelaksanaan Audit Keamanan SPBE;

(4) Jadwal pelaksanaan Audit Keamanan SPBE;

(5) Hasil penilaian mandiri Keamanan Informasi; dan

(6) Hasil penilaian evaluasi SPBE.

2) Perencanaan, dengan uraian berupa:

a) Perencanaan Audit Keamanan SPBE dilakukan oleh Tim Audit Keamanan SPBE dengan menyusun perencanaan Audit Keamanan SPBE.

b) Perencanaan Audit Keamanan SPBE mencakup:

(1) Analisis risiko keamanan SPBE;

(2) Penentuan kriteria Audit Keamanan SPBE; dan

(3) Rencana pengujian Audit Keamanan SPBE.

c) Analisis risiko keamanan SPBE dilakukan melalui proses identifikasi dan evaluasi risiko keamanan SPBE yang relevan dengan lingkup Audit Keamanan SPBE.

d) Penentuan kriteria Audit Keamanan SPBE dilakukan melalui proses identifikasi dan pemetaan kriteria kontrol Keamanan SPBE yang sesuai dengan lingkup Audit Keamanan SPBE.

e) Rencana pengujian Audit Keamanan SPBE berisikan rencana prosedur pengujian yang harus dilakukan Auditor atas kontrol Keamanan SPBE termasuk alokasi waktu, personel dan alat bantu Audit Keamanan SPBE.

f) Dalam melakukan perencanaan Audit Keamanan SPBE, Tim Audit dapat memperhatikan Laporan Hasil Audit sebelumnya.

3) Pelaksanaan, dengan uraian berupa:

a) Pelaksanaan Audit Keamanan SPBE paling sedikit mencakup prosedur:

(1) Pemahaman kontrol Keamanan SPBE;

(2) Evaluasi desain kontrol Keamanan SPBE;

(3) Evaluasi implementasi kontrol Keamanan SPBE; dan
(4) Evaluasi efektivitas kontrol Keamanan SPBE.

b) Pemahaman kontrol Keamanan SPBE dilakukan melalui prosedur yang dilakukan Auditor dalam mengidentifikasi informasi terdokumentasi untuk memperoleh pemahaman yang memadai tentang kontrol Keamanan SPBE.

c) Evaluasi desain kontrol Keamanan SPBE dilakukan melalui prosedur yang dilakukan Auditor untuk memperoleh keyakinan yang memadai bahwa desain kontrol Keamanan SPBE telah sesuai dengan kriteria kontrol Keamanan SPBE yang digunakan.

d) Pengujian implementasi kontrol Keamanan SPBE dilakukan melalui prosedur yang dilakukan Auditor untuk memperoleh keyakinan yang memadai bahwa implementasi kontrol telah sesuai dengan desain kontrol yang ada.

e) Pengujian terinci efektivitas pengendalian Keamanan SPBE dilakukan melalui prosedur yang dilakukan Auditor untuk:
(1) Memperoleh keyakinan yang memadai bahwa kontrol Keamanan SPBE telah dapat mencapai tujuannya dengan efektif; atau
(2) Mengidentifikasi risiko yang terjadi karena adanya kelemahan desain dan/atau implementasi kontrol Keamanan SPBE.

f) Tim Audit Keamanan SPBE menggunakan Pertimbangan Profesional untuk menentukan simpulan dari hasil prosedur:
(1) Evaluasi desain kontrol Keamanan SPBE;
(2) Pengujian implementasi kontrol Keamanan SPBE; dan
(3) Pengujian terinci efektivitas kontrol Keamanan SPBE.

g) Simpulan dari hasil prosedur evaluasi desain kontrol Keamanan SPBE terdiri atas:
(1) Memadai;
(2) Perlu peningkatan; atau
(3) Tidak memadai.

h) Simpulan menentukan prosedur Audit Keamanan SPBE setelah evaluasi desain kontrol Keamanan SPBE, yaitu:

(1) Jika memadai, maka Tim Audit Keamanan SPBE melakukan prosedur pengujian implementasi kontrol Keamanan SPBE dengan cakupan uji petik yang cukup;

(2) Jika perlu peningkatan, maka Tim Audit Keamanan SPBE melakukan prosedur pengujian implementasi kontrol Keamanan SPBE dengan cakupan uji petik yang ekstensif; atau

(3) Jika tidak memadai, maka Tim Audit Keamanan SPBE tidak perlu melakukan prosedur pengujian implementasi kontrol keamanan SPBE dan langsung melakukan prosedur pengujian terinci efektivitas kontrol Keamanan SPBE.

i) Simpulan dari hasil prosedur evaluasi desain kontrol Keamanan SPBE terdiri atas:

(1) Sesuai dengan desain kontrol; atau

(2) Tidak sesuai dengan desain kontrol.

j) Simpulan menentukan prosedur Audit Keamanan SPBE setelah pengujian implementasi kontrol Keamanan SPBE yaitu:

(1) Jika sesuai dengan desain kontrol, maka Tim Audit Keamanan SPBE melakukan prosedur pengujian terinci efektivitas kontrol Keamanan SPBE dengan cakupan uji petik yang cukup; atau

(2) Jika tidak sesuai dengan desain kontrol, maka Tim Audit Keamanan SPBE melakukan penambahan cakupan uji petik dalam evaluasi implementasi pengendalian Keamanan SPBE dan harus melakukan prosedur pengujian terinci efektivitas kontrol Keamanan SPBE dengan cakupan uji petik yang ekstensif.

k) Simpulan dari hasil prosedur pengujian terinci efektivitas kontrol Keamanan SPBE terdiri atas:

(1) Efektif;

(2) Perlu peningkatan; atau

(3) Belum efektif.

4) Supervisi, dengan uraian berupa

a) Supervisi Audit Keamanan SPBE mencakup:

(1) Supervisi aspek mutu Audit Keamanan SPBE; dan
(2) Supervisi aspek teknis Audit Keamanan SPBE.

b) Supervisi aspek mutu Audit Keamanan SPBE dilakukan melalui prosedur yang dilakukan oleh Tim Audit Keamanan SPBE untuk memastikan bahwa pelaksanaan setiap Audit Keamanan SPBE telah sesuai dengan pedoman kendali mutu Audit Keamanan SPBE yang dimiliki oleh Inspektorat.

c) Supervisi aspek teknis Audit Keamanan SPBE dilakukan melalui prosedur yang dilakukan oleh Tim Audit Keamanan SPBE untuk memastikan bahwa pelaksanaan setiap Audit Keamanan SPBE telah memadai secara teknis sesuai dengan lingkup Audit Keamanan SPBE.

d) Supervisi Audit Keamanan SPBE dilakukan sesuai dengan metodologi dan sumber daya yang dimiliki Inspektorat.

5) Pelaporan, dengan uraian berupa:

a) Pelaporan Audit Keamanan SPBE dilakukan oleh Tim Audit Keamanan SPBE dengan menyusun laporan hasil audit.

b) Laporan hasil audit mencakup:
(1) Kondisi yang memerlukan perhatian pimpinan Unit Organisasi selaku *Auditee*;
(2) Risiko atau potensi risiko yang diidentifikasi;
(3) Kriteria kontrol Keamanan SPBE yang digunakan sesuai dengan lingkup Audit Keamanan SPBE;
(4) Rekomendasi tindakan perbaikan yang dapat dilakukan oleh Unit Organisasi sebagai *Auditee*; dan
(5) Rencana tindak lanjut Unit Organisasi selaku *Auditee*.

c) Kondisi yang memerlukan perhatian pimpinan Unit Organisasi selaku *Auditee* harus mencakup:
(1) Kelemahan dalam desain kontrol Keamanan SPBE dibandingkan dengan kriteria kontrol Keamanan SPBE yang digunakan; dan
(2) Ketidaksesuaian antara implementasi kontrol Keamanan SPBE dengan desain kontrol Keamanan SPBE.

d) Risiko atau potensi risiko yang diidentifikasi terdiri atas:
(1) Kelemahan desain dan/atau implementasi kontrol Keamanan SPBE; dan

(2) Hasil pelaksanaan pengujian terinci kontrol Keamanan SPBE.

e) Rekomendasi tindakan perbaikan yang dapat dilakukan oleh *Auditee* dilakukan untuk meningkatkan:
   (1) Kecukupan desain kontrol Keamanan SPBE;
   (2) Kesesuaian implementasi kontrol Keamanan SPBE; dan
   (3) Efektivitas kontrol Keamanan SPBE.

KEPALA LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH,

ttd

HENDRAR PRIHADI