



PEMERINTAH KABUPATEN BULELENG
SEKRETARIAT DAERAH

Jl. Pahlawan No. 1 Telp. (0362) 21985
Singaraja

Singaraja, 7 Juli 2023

Kepada
Yth. Para Kepala Perangkat Daerah
Lingkup Pemkab. Buleleng
di -
Singaraja

SURAT EDARAN

Nomor : 400.13.53/ 1853 /T.Kelola.Kominfosanti/VII/2023

TENTANG

**PEDOMAN PENYELENGGARAAN AUDIT TEKNOLOGI INFORMASI DAN
KOMUNIKASI (TIK) LINGKUP PEMERINTAH
KABUPATEN BULELENG**

Menindaklanjuti instruksi Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik dan Peraturan Bupati Buleleng Nomor 58 Tahun 2019 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik (SPBE) khususnya terkait Audit Teknologi Informasi dan Komunikasi (TIK), maka untuk memberikan pemahaman yang sarna standar kerangka kerja Audit TIK dan memberikan pedoman penyelenggaraan Audit TIK dengan ini disampaikan Surat Edaran tentang Pedoman Penyelenggaraan Audit Teknologi Informasi dan Komunikasi (TIK) Lingkup Pemerintah Kabupaten Buleleng (*pedoman terlampir*).

Demikian untuk menjadi perhatian dan dipedomani.



Tembusan :

1. PJ. Bupati Buleleng, sebagai laporan;
2. Arsip.



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

LAMPIRAN SURAT SEKRETARIS DAERAH
KABUPATEN BULELENG
NOMOR 400.13.53/1853/T.Kelola.Kominfosanti/VII/2023
TENTANG
PEDOMAN PENYELENGGARAAN AUDIT TEKNOLOGI
INFORMASI DAN KOMUNIKASI (TIK) LINGKUP
PEMERINTAH KABUPATEN BULELENG

TAHAPAN PENYELENGGARAAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI
(TIK) LINGKUP PEMERINTAH KABUPATEN BULELENG

BAB I
STANDAR PELAKSANAAN AUDIT SPBE

Standar pelaksanaan Audit TIK adalah Batasan minimal bagi regulator dan auditor untuk membantu pelaksanaan audit sesuai prosedur dalam rangka pencapaian tujuan audit.

Standar Pelaksanaan Audit TIK memiliki tujuan sebagai berikut:

- a. Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit TIK;
- b. Menyusun Kerangka Kerja dalam pemberian layanan jasa Audit TIK, guna menambah nilai kepada yang diaudit (Auditee) melalui perbaikan proses dan operasionalnya; dan
- c. Menyusun dasar dalam melakukan evaluasi terhadap regulasi dan pelaksanaan Audit TIK guna mendorong rencana perbaikan.

Standar Pelaksanaan Audit TIK mencakup hal-hal sebagai berikut:

1.1 Standar Umum;

- a. Standar Umum memberikan prinsip dasar untuk mengatur Auditor TIK dalam melaksanakan tugasnya dan sehingga pelaksanaan pekerjaan Audit TIK hingga pelaporannya dapat terlaksana dengan baik dan efektif.
- b. Dalam rangka memastikan kehandalan dan keamanan sistem teknologi informasi dan komunikasi di lingkungan Pemerintah Kabupaten Buleleng perlu dilakukan audit TIK secara berkala dan berkelanjutan
- c. Objek Audit TIK tersebut terdiri dari :
 1. Infrastruktur SPBE yang terdiri dari Pusat Data, Jaringan Intra Pemerintah Kabupaten Buleleng dan Sistem Penghubung Layanan Pemerintah Kabupaten Buleleng;



2. Aplikasi SPBE Pemerintah Kabupaten Buleleng, yang merupakan aplikasi khusus yang dikembangkan, dikelola dan/atau digunakan oleh Perangkat Daerah guna mendukung uraian tugas pokok dan fungsi serta memenuhi kebutuhan khusus Perangkat Daerah; dan
 3. Keamanan infrastruktur dan keamanan aplikasi SPBE Pemerintah Kabupaten Buleleng yang terkait pada poin a dan b diatas.
- d. Lingkup cakupan Audit TIK yang dilaksanakan meliputi pemeriksaan hal pokok teknis pada setiap objek audit yaitu :
1. penerapan tata kelola dan manajemen teknologi informasi dan komunikasi;
 2. fungsionalitas teknologi informasi dan komunikasi;
 3. kinerja teknologi informasi dan komunikasi yang dihasilkan; dan
 4. aspek teknologi informasi dan komunikasi lainnya.
- e. Permintaan Audit TIK diajukan untuk satu atau lebih dari tujuan berikut ini:
1. Peningkatan kinerja birokrasi dan pelayanan publik;
 2. Penilaian kesesuaian dengan standar/prosedur/pedoman dan kesesuaian dengan rencana/kebutuhan/kondisi;
 3. Identifikasi status teknologi yang dimiliki, identifikasi kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
 4. Perencanaan pengembangan sistem/teknologi dan perencanaan perbaikan kelemahan; dan/atau
 5. Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.
- f. Audit TIK di lingkungan Pemerintah Kabupaten Buleleng terdiri atas audit Internal dan Eksternal
1. Audit eksternal TIK dilaksanakan oleh lembaga pelaksana Audit TIK pemerintah atau lembaga pelaksana Audit TIK yang terakreditasi dan auditor yang tersertifikasi sesuai dengan ketentuan peraturan perundang-undangan. Sebelum dilakukan audit eksternal TIK pada Pemerintah Kabupaten Buleleng, harus terlebih dahulu melaksanakan audit internal TIK Pemerintah Kabupaten Buleleng.
 2. Audit internal TIK dilaksanakan oleh tim auditor internal TIK Pemerintah Kabupaten Buleleng yang mempunyai kompetensi teknis sesuai objek audit dan lingkup audit dan ditetapkan oleh Sekretaris Daerah selaku Koordinator SPBE Pemerintah Kabupaten Buleleng. Audit internal TIK dapat dilakukan dengan bantuan tenaga ahli audit TIK yang tersertifikasi atau lembaga audit TIK yang terakreditasi, dengan :

- 1) memastikan bahwa tenaga ahli yang digunakan mempunyai kompetensi, kualifikasi profesi, pengalaman yang relevan, dan independensi; dan
 - 2) melakukan evaluasi terhadap hasil kerja tenaga ahli yang digunakan dan menyimpulkan tingkatan ketergunaannya.
- g. Tujuan, wewenang dan tanggung jawab suatu aktivitas Audit TIK harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam audit (*audit charter*), surat tugas, atau dokumen-dokumen yang setara. Hal yang perlu diperhatikan sebagai berikut:
- 1) Surat tugas atau piagam audit (*audit charter*) menjelaskan tujuan audit, ruang lingkup, kewenangan tim audit dan etika yang harus dipatuhi oleh tim audit.
 - 2) Penugasan Tim Auditor TIK dalam melaksanakan Audit TIK berupa Surat Tugas yang diberikan oleh Sekretaris Daerah selaku Koordinator SPBE Pemerintah Kabupaten Buleleng dan ditembuskan kepada Dinas teknis terkait TIK dan Auditee.
 - 3) Kegiatan Audit TIK dilakukan berdasarkan uraian yang disusun di dalam surat penugasan kerja Audit TIK. Surat penugasan kerja Audit TIK berisikan antara lain:
 1. Tujuan Audit TIK;
 2. Lingkup Audit TIK;
 3. Wewenang auditor;
 4. Tanggung jawab auditor;
 5. Periode penugasan; dan
 6. Tata pelaporan hasil Audit TIK.
- h. Integritas Auditor TIK diwujudkan melalui sikap independen, objektif, dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor TIK dituntut untuk menjalankan hal-hal sebagai berikut:
- 1) Menggunakan keahlian profesionalnya dengan cermat dan seksama (*due professional care*) serta berhati-hati (*prudent*) dalam setiap penugasan;
 - 2) Senantiasa mengasah dan melatih kecermatan profesionalnya;
 - 3) Meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan;
 - 4) Mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
 - 5) Memiliki pengetahuan (*knowledge*), keterampilan (*skill*), sikap (*attitude*) dan pengalaman (*experience*) yang sesuai /guna memenuhi tanggung jawabnya dalam pelaksanaan audit.

1.2 Standar Pelaksanaan;

a. Tim Audit TIK terdiri dari posisi-posisi dengan uraian tugas dan tanggung jawab sebagai berikut:

1. Ketua Tim Audit (*Lead Auditor*), bertanggung jawab merencanakan Audit TIK, melaksanakan Audit TIK di lapangan, mengendalikan data dan melaporkan hasil Audit TIK serta secara efektif mengelola aktivitas audit untuk menjamin agar tujuan Audit TIK tercapai.

Ketua tim audit (*Lead Auditor*) harus melakukan hal-hal sebagai berikut:

- 1) Menyusun dan menetapkan rencana audit (*audit plan*) guna menentukan prioritas-prioritas dalam kegiatan Audit TIK yang konsisten dengan tujuan audit sesuai dengan piagam audit (*audit charter*);
 - 2) Menyampaikan rencana audit (*audit plan*) kepada Auditee untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumberdaya;
 - 3) Mengelola sumber daya audit yang tepat, memadai, dan efektif untuk melaksanakan rencana audit yang telah disetujui;
 - 4) Melakukan koordinasi dengan pimpinan Lembaga Audit TIK (LATIK) untuk menjamin bahwa pelaksanaan Audit TIK dapat berjalan efektif dan efisien; dan
 - 5) Memberi laporan yang memadai kepada pimpinan unit kerja yang diaudit mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.
2. Auditor, bertugas membantu *Lead Auditor* dalam aktivitas Audit TIK;
 3. Asisten Auditor, bertugas membantu Auditor dalam aktivitas Audit TIK. Asisten Auditor harus sudah mengikuti sosialisasi Audit TIK;
 4. Teknisi, bertugas membantu Auditor dalam pengumpulan data lapangan;
 5. Pengawas Mutu, berperan melakukan monitoring dan evaluasi aktivitas Audit TIK untuk menjamin pelaksanaan Audit TIK sesuai dengan ketentuan peraturan perundang-undangan. Pengawas mutu dapat berasal dari pihak eksternal; dan
 6. Narasumber, berperan memberi masukan yang berkaitan dengan isu, status industri dan teknologi, serta keilmuan yang relevan dengan lingkup yang diaudit.

Dalam pelaksanaan suatu Audit TIK, Tim Audit TIK minimal terdiri dari seorang Ketua Tim Audit (*Lead Auditor*) dan Auditor.

b. Pemeriksaan yang dilakukan terhadap Auditee mencakup:

1. Penerapan tata kelola dan manajemen SPBE;
2. Fungsionalitas dan kinerja SPBE; dan
3. Tingkat kepatuhan terhadap regulasi.

- c. Hal yang perlu diperhatikan dalam Perencanaan Audit TIK sebagai berikut:
1. Auditor harus menyusun perencanaan dan program Audit TIK berdasarkan pendekatan risiko (*risk approach*). Hasil penilaian risiko digunakan untuk mengatur prioritas dan pengalokasian sumber daya audit.
 2. Dalam melakukan penilaian risiko, Audit TIK paling sedikit melakukan beberapa hal sebagai berikut:
 - 1) Mengidentifikasi aset SPBE yang berupa data, aplikasi SPBE, sistem operasi, infrastruktur SPBE, fasilitas, dan personil;
 - 2) Mengidentifikasi kegiatan dan proses bisnis yang menggunakan SPBE; dan
 - 3) Mengidentifikasi tingkat dampak risiko SPBE dalam operasional layanan SPBE dan mempertimbangkan skala prioritas berdasarkan tingkat risiko.
 3. Program Audit TIK disusun sesuai dengan cakupan Audit TIK yang sudah ditetapkan dari hasil penilaian risiko TIK. Auditor dapat mengalokasikan sumber daya yang lebih fokus pada area yang berisiko tinggi dan mempunyai skala kepentingan yang tinggi pada Layanan TIK.
 4. Rencana kerja Audit TIK harus disusun untuk setiap penugasan Audit TIK. Dalam hal merencanakan Audit TIK, Auditor harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit, yang paling sedikit mencakup:
 - 1) Tujuan Audit TIK, jadwal, jumlah auditor, dan pelaporan;
 - 2) Lingkup Audit TIK sesuai hasil penilaian risiko;
 - 3) Pembagian tugas dan tanggung jawab dari auditor; dan
 - 4) Alokasi sumber daya.
 5. Rencana audit (*audit plan*) disusun dengan mempertimbangkan, antara lain:
 - 1) Sistem pengendalian internal dan kepatuhan Auditee terhadap kebijakan atau standar;
 - 2) Penetapan tujuan Audit TIK;
 - 3) Penetapan kecukupan lingkup; dan
 - 4) Penggunaan metodologi yang tepat.
 6. Ketua tim audit dan Auditee harus menyetujui rencana audit sebelum tahap pelaksanaan audit.
- d. Hal yang perlu diperhatikan dalam Pelaksanaan Audit TIK sebagai berikut:
1. Proses pelaksanaan Audit TIK mengacu pada program Audit TIK yang telah disusun pada tahap perencanaan
 2. Auditor menyiapkan kertas kerja Audit TIK untuk mendokumentasikan pelaksanaan Audit TIK. Dokumen kertas kerja Audit TIK, yang sekurangnya terdiri dari:

- 1) Dokumen rencana dan program audit;
 - 2) Surat Tugas Tim Audit;
 - 3) Laporan Hasil Audit; dan
 - 4) Laporan Tindak Lanjut Hasil Audit.
3. 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:
- 1) Memperoleh bukti-bukti audit yang cukup, handal, dan relevan untuk mendukung penilaian audit dan kesimpulan audit;
 - 2) Mendasarkan temuan dan kesimpulan audit pada analisis dan interpretasi yang memadai atas bukti-bukti audit;
 - 3) Menyiapkan, mengelola dan menyimpan data dan informasi yang diperoleh selama pelaksanaan audit; dan
 - 4) Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
4. Dalam hal komunikasi atas hasil Audit TIK, Auditor TIK harus mengkomunikasikan hasil pelaksanaan audit kepada pihak-pihak yang berkepentingan. Komunikasi tersebut harus mencakup tujuan dan ruang lingkup pelaksanaan audit, selain kesimpulan yang terkait, rekomendasi dan rencana tindak lanjut. Jika komunikasi final berisi kesalahan atau penghilangan yang signifikan, ketua tim audit (*Lead Auditor*) harus mengkomunikasikan informasi yang telah diperbaiki kepada semua pihak yang menerima komunikasi.
- e. Monitoring dan evaluasi dilakukan oleh pengawas mutu dalam rangka memberikan informasi atas aktivitas audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam pelaksanaan audit, serta memastikan audit diimplementasikan secara efektif. Pengawas mutu menyampaikan hasil monitoring dan evaluasi aktivitas audit kepada Walikota dan koordinator SPBE.
- f. 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.
- g. Aspek monitoring dalam aktivitas Audit TIK meliputi:
1. Kepatuhan terhadap Kode Etik dan Standar Audit;
 2. Kesesuaian terhadap Piagam Audit;
 3. Kesesuaian terhadap Rencana Audit; dan
 4. Kesesuaian terhadap Protokol Audit

1.3 Standar Pelaporan

- a. Laporan audit disampaikan oleh ketua Tim audit kepada Auditee dan pimpinan Aparat pengawasan Intern Pemerintah (APIP) untuk memutuskan apakah kesimpulan hasil pemeriksaan, termasuk temuan yang diperoleh selama Audit TIK berlangsung, serta rekomendasi yang diberikan dapat diterima oleh Auditee.
- b. Hal yang diperhatikan dalam pelaporan audit sebagai berikut:
 1. Laporan hasil audit dibuat dalam bentuk dokumen laporan audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas;
 2. Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh auditee secara tertulis dari pejabat auditee yang bertanggung jawab;
 3. Setelah konfirmasi dilakukan, Tim Audit wajib menyampaikan laporan hasil audit yang berisikan antara lain:
 - 1) Tujuan Audit TIK;
 - 2) Lingkup Audit TIK;
 - 3) Periode pelaksanaan Audit TIK;
 - 4) Kriteria dan acuan Audit TIK;
 - 5) Metoda pengumpulan data dan metode analisa;
 - 6) Hasil analisis, kesimpulan, dan rekomendasi;
 - 7) Tanggapan Auditee terhadap hasil Audit TIK;
 - 8) Batasan dan kendala yang ditemui selama proses Audit TIK; dan
 - 9) Tata cara pendistribusian laporan sesuai dengan surat penugasan.
 4. Draft laporan diriviu oleh ketua tim audit untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit.
 5. Laporan Audit diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli. Pada setiap halaman dokumen laporan hasil audit diberi identifikasi (nomor dokumen) yang menggambarkan sekurang kurangnya: tahun pelaksanaan audit, nomor urut atau nomor seri dokumen, domain Aplikasi atau Infrastruktur SPBE, Auditee dan kode pengendalian distribusi salinan dokumen.
 6. Laporan Audit didistribusikan kepada Bupati.
 7. Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh Bupati kepada Instansi Pemerintah Pusat, paling sedikit satu kali dalam 2 tahun.



1.4 Standar Tindak Lanjut.

- a. Dalam kondisi pemantauan terhadap tindak lanjut akan dilaksanakan, ketua tim audit (*Lead Auditor*) harus menetapkan sebuah sistem pemantauan terhadap tindak lanjut temuan, kesimpulan dan rekomendasi audit oleh Auditee, mencakup cara berkomunikasi dengan Auditee, prosedur pemantauan, dan laporan status temuan.
- b. Untuk menjamin pelaksanaan tindak lanjut hasil audit TIK, APIP melakukan:
 1. pemantauan tindak lanjut hasil audit TIK;
 2. koordinasi dengan Koordinator SPBE, Dinas teknis terkait TIK, Auditee dan pihak terkait lainnya untuk mendorong penyelesaian Tindak Lanjut Hasil Audit;
 3. Tindak lanjut perbaikan dari Auditee perlu dievaluasi oleh auditor, untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi Auditee;
 4. APIP dan Auditee harus memelihara dokumentasi atas hasil tindak lanjut tersebut.

BAB II

PANDUAN TEKNIS AUDIT TIK

2.1 Tata Cara Pelaksanaan Audit

Pelaksanaan Audit SPBE terbagi dalam tiga kelompok tahapan, yaitu:

- a. tahap Perencanaan (*Pre – Audit*);
- b. tahap Pelaksanaan Lapangan (*onsite audit*); dan
- c. tahap Analisa data dan pelaporan (*post audit*).

Tata laksana dalam tiga tahapan diatas sebagai berikut:

1. Penyiapan tim pelaksana meliputi penetapan personil tim audit.
2. *Quick Assessment* dilakukan untuk mengenali obyek audit dengan mengidentifikasi isu terkini (*current issue*), lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, proses bisnis dari organisasi, atau bagian yang diaudit, teknologi produk (bila relevan), teknologi proses (bila relevan), pengguna produk (bisa relevan).
3. Penyiapan protocol audit

Penyiapan protocol audit dimulai dengan komunikasi dengan auditee untuk menjelaskan secara garis besar tentang audit TIK. Tim auditor menindaklanjuti dengan menyusun protokol audit yang berisi detail instrumen audit, meliputi tujuan, lingkup, kriteria, acuan, metode pengumpulan data, metoda Analisa, perkiraan jadwal pelaksanaan, Daftar data,

pertanyaan dan pengujian, Formulir untuk mencatat data, jawaban, hasil observasi dan hasil pengujian.

4. Penyelesaian protocol audit.

Komunikasi lanjutan dengan auditee dilakukan untuk menyepakati protocol yang disusun. Auditee dapat memberi masukan untuk memperbaiki protocol dan menunjuk personil di pihak auditee yang akan mendampingi auditor dalam pelaksanaan lapangan. Dokumen protocol ditandatangani oleh penanggung jawab tim auditor dan penanggung jawab tim auditee.

5. Penyiapan kertas kerja dan penyiapan *audit tools*

Setelah protocol audit disepakati, tim auditor menyiapkan secara rinci form-form yang diperlukan. Form tersebut dianggap sebagai kerja kerja formal dalam pengumpulan data.

6. Melakukan pertemuan pembukaan dengan auditee

Pelaksanaan lapangan diawasi dengan pertemuan pembukaan yang memaparkan rincian pelaksanaan lapangan audit aplikasi TIK dengan diawali dengan tata cara pelaksanaan audit melalui.

7. Melaksanakan audit lapangan, melalui:

- 1) Penelaahan dokumen;
- 2) Wawancara;
- 3) Observasi lapangan;
- 4) Pengujian; dan
- 5) Verifikasi bukti. Auditor dapat meminta data atau informasi guna keperluan pelaksanaan tugas, baik dalam bentuk salinan cetak maupun salinan lunak termasuk basis data dari Aplikasi SPBE

8. Melakukan analisis bukti;

9. Memberikan rekomendasi perbaikan untuk mengatasi temuan audit TIK. Temuan Audit TIK merupakan keadaan dimana fakta status penyelenggaraan SPBE Auditee tidak sesuai dengan ketentuan peraturan perundang-undangan serta standar penyelenggaraan SPBE.

10. Melakukan pertemuan penutupan dengan auditee;

11. Penyusunan laporan;

12. Proof-read laporan (memeriksa kembali laporan hasil audit);

13. Penyerahan laporan; dan

14. Evaluasi aktivitas



2.2 Pedoman Teknis Audit Infrastruktur SPBE

- a. Audit TIK Infrastruktur SPBE dengan obyek pusat data, jaringan intra dan sistem penghubung layanan, dilakukan pada aspek:
 1. Tata kelola infrastruktur SPBE, yang meliputi evaluasi, pengarahan, dan pemantauan;
 2. Manajemen Infrastruktur SPBE, yang meliputi
 - 1) Manajemen keamanan,
 - 2) Manajemen risiko,
 - 3) Manajemen asset,
 - 4) Manajemen pengetahuan,
 - 5) Manajemen sumber daya manusia (SDM),
 - 6) Manajemen layanan,
 - 7) Manajemen perubahan; dan
 - 8) Manajemen data.
 - b. Fungsionalitas dan kinerja operasional dan pemeliharaan Infrastruktur SPBE, yang meliputi perencanaan, pengembangan, pengoperasian, dan pemeliharaan infrastruktur SPBE; dan
 - c. Tingkat kepatuhan terhadap regulasi.
- b. Auditor melakukan pemeriksaan terhadap Infrastruktur SPBE untuk memastikan bahwa:
 1. Perubahan teknologi, ketentuan hukum, dan regulasi dipantau;
 2. Strategi Infrastruktur SPBE dan rencana Infrastruktur SPBE sudah selaras dengan kebutuhan Perangkat Daerah;
 3. Standar teknologi sudah ditetapkan dan diimplementasikan;
 4. Rekomendasi arsitektur Infrastruktur SPBE sudah dilaksanakan;
 5. Rencana pengadaan Infrastruktur SPBE sudah mempertimbangkan faktor risiko, biaya, manfaat, keamanan, dan kesesuaian teknis dengan Infrastruktur SPBE lainnya;
 6. Pengadaan Infrastruktur SPBE sesuai dengan rencana;
 7. Aset SPBE sudah diidentifikasi, ditentukan pemilik atau penanggung jawabnya, dan dicatat agar dapat dilindungi secara tepat;
 8. Penghapusan aset SPBE sudah dilakukan dengan tepat sehingga aset aman untuk dihapus dan/atau dimusnahkan;
 9. Kapasitas Infrastruktur SPBE sudah direncanakan dengan baik, dipantau, dianalisis dan dievaluasi penggunaannya;
 10. Insiden terkait Infrastruktur SPBE dicatat dan ditangani dengan baik sesuai dengan kesepakatan tingkat layanan;

11. Pemeliharaan Infrastruktur SPBE telah dilakukan secara reguler sesuai dengan petunjuk penggunaannya; dan
 12. Setiap pegawai/petugas pengelola fasilitas, Infrastruktur SPBE harus memiliki kompetensi yang sesuai dengan bidang tugasnya.
- c. Audit dapat difokuskan pada penilaian fungsionalitas dan kinerja infrastruktur SPBE.
 - d. Auditor harus melakukan pemeriksaan terhadap penyediaan layanan infrastruktur SPBE oleh pihak eksternal untuk memastikan bahwa :
 1. Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;
 2. Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
 3. Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan
 4. Perjanjian Kerahasiaan (*Non Disclosure Agreement*) telah ditandatangani oleh pihak eksternal.
 - e. Panduan teknis dan kriteria penilaian pada audit infrastruktur SPBE dapat ditetapkan lebih lanjut oleh APIP, sesuai ketentuan peraturan perundang-undangan.

2.3 Pedoman Teknis Audit Aplikasi SPBE

- a. Audit Aplikasi SPBE dilakukan pada aspek:
 1. Penerapan tata kelola Aplikasi SPBE yang meliputi evaluasi, pengarahan, dan pemantauan;
 2. Penerapan manajemen Aplikasi SPBE, yang meliputi
 - 1) Manajemen keamanan,
 - 2) Manajemen risiko,
 - 3) Manajemen asset,
 - 4) Manajemen pengetahuan,
 - 5) Manajemen sumber daya manusia,
 - 6) Manajemen layanan,
 - 7) Manajemen perubahan, dan
 - 8) Manajemen data;
 3. Fungsionalitas dan Kinerja Aplikasi SPBE yang meliputi perencanaan, pengembangan, pengoperasian, dan pemeliharaan aplikasi SPBE; dan
 4. Tingkat kepatuhan terhadap regulasi.
- b. Auditor harus melakukan pemeriksaan terhadap Arsitektur Aplikasi SPBE paling sedikit untuk memastikan bahwa:



1. Aplikasi direncanakan dalam suatu dokumen spesifikasi kemampuan aplikasi (*Software Requirements Specifications*) dengan mengacu kepada arsitektur SPBE Nasional, arsitektur SPBE Pemerintah Kabupaten Buleleng, dengan mempertimbangkan kebutuhan, peluang dan proses bisnis
 2. Perubahan kebutuhan dan proses bisnis dipantau;
 3. Standar pembangunan dan pengembangan Aplikasi SPBE sudah ditetapkan dan diimplementasikan;
 4. Rekomendasi arsitektur Aplikasi SPBE sudah dilaksanakan.
 5. Aplikasi SPBE sudah dibangun dan dikembangkan sesuai rencana dengan metodologi pembangunan dan pengembangan yang ada;
 6. Rancangan Aplikasi SPBE sudah mempertimbangkan kebutuhan keamanan dan ketersediaan;
 7. Aplikasi SPBE memiliki dokumentasi pembangunan dan pengembangan Aplikasi SPBE yang dibutuhkan;
 8. Aplikasi SPBE sudah diujicobakan sebelum dioperasionalkan sesuai dengan kebutuhannya. Uji coba terhadap aplikasi harus terdokumentasi.
 9. Pengendalian akses ke kode sumber (*source code*) Aplikasi SPBE sudah dilakukan;
 10. Pelatihan kepada pengguna dan pegawai/petugas pengelola Aplikasi SPBE telah dilakukan;
 11. Tinjauan pasca implementasi telah dilakukan ketika selesai implementasi Aplikasi SPBE.
 12. Kapasitas Aplikasi SPBE sudah direncanakan dengan baik, dipantau, dianalisis dan dievaluasi penggunaannya;
 13. Insiden terkait Aplikasi SPBE dicatat dan ditangani dengan baik sesuai dengan kesepakatan tingkat layanan;
 14. Pengoperasian dan pemeliharaan Aplikasi SPBE telah dilakukan secara rutin sesuai dengan pedoman; dan
 15. Setiap pegawai/petugas pengelola Aplikasi SPBE harus mempunyai kompetensi yang sesuai dengan bidang tugasnya.
- c. Auditor harus melakukan pemeriksaan terhadap penyediaan layanan pengembangan dan/atau pemeliharaan aplikasi SPBE oleh pihak ketiga, paling sedikit untuk memastikan bahwa:
1. Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;
 2. Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
 3. Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan

4. Perjanjian Kerahasiaan (*Non Disclosure Agreement*) telah ditandatangani oleh pihak eksternal.
- d. Panduan teknis dan kriteria penilaian pada audit aplikasi SPBE dapat ditetapkan lebih lanjut oleh APIP, sesuai ketentuan peraturan perundang-undangan.

2.4 Pedoman Teknis Audit Keamanan SPBE

- a. Audit Keamanan SPBE dilakukan pada aspek:
 1. Penerapan tata kelola keamanan pada lingkup aplikasi dan infrastruktur SPBE, yang meliputi evaluasi, pengarahan, dan pemantauan;
 2. Penerapan manajemen keamanan SPBE, yang meliputi: kebijakan keamanan; organisasi keamanan; keamanan personil; keamanan aset; keamanan akses; keamanan kriptografi; keamanan fisik dan lingkungan; keamanan operasional; keamanan komunikasi; keamanan pengembangan dan pemeliharaan; keamanan rekanan; insiden keamanan; keamanan kontinuitas; dan/atau kepatuhan keamanan;
 3. Kinerja Keamanan Aplikasi SPBE dan Keamanan Infrastruktur SPBE; dan
 4. Tingkat kepatuhan terhadap regulasi.
- b. Auditor harus melakukan pemeriksaan terhadap Arsitektur Keamanan SPBE paling sedikit untuk memastikan bahwa:
 1. Perubahan ancaman, kerentanan, risiko, dan kendali SPBE dipantau;
 2. Strategi Keamanan SPBE dan rencana Keamanan SPBE sudah selaras dengan kebutuhan Pemerintah Kabupaten Buleleng;
 3. Standar keamanan informasi sudah ditetapkan dan diimplementasikan; dan
 4. Rekomendasi arsitektur Keamanan SPBE sudah dilaksanakan.
 5. Peta Rencana Keamanan SPBE telah disusun berdasarkan analisis risiko dan kesenjangan arsitektur Keamanan SPBE;
 6. Peta Rencana Keamanan SPBE disusun berdasarkan prioritas pengembangannya;
 7. Sejauh mana Peta Rencana Keamanan SPBE sudah diimplementasikan;
 8. Peta Rencana Keamanan SPBE ditinjau secara berkala berdasarkan kajian risiko, rencana anggaran, atau hasil evaluasi SPBE.
 9. Kebijakan dan pedoman keamanan informasi sudah disusun dan disosialisasikan secara berkala;
 10. Dilakukan pelatihan peningkatan kepedulian (*awareness training*) keamanan informasi secara berkala;
 11. Pengelola dan pelaksana keamanan informasi sudah ditetapkan; dan
 12. Setiap sistem, Aplikasi SPBE, dan data telah ditentukan tingkat kritikalitasnya;



13. Setiap sistem dan proses bisnis telah ditetapkan pemiliknya;
 14. Ada prosedur pengelolaan pengguna dan hak aksesnya untuk setiap pegawai dan pihak eksternal;
 15. Setiap pengguna sistem diberi hak akses sesuai dengan kebutuhan minimumnya dan disetujui oleh pemilik proses bisnis;
 16. Setiap pengguna sistem bisa diidentifikasi secara individual;
 17. Dilakukan tinjauan secara berkala terhadap pengguna dan hak aksesnya di setiap sistem;
 18. Dilakukan pemantauan keamanan sistem secara proaktif;
 19. Dilakukan pengujian keamanan sistem secara berkala;
 20. Insiden keamanan informasi ditangani secara efektif;
 21. Dilakukan perlindungan terhadap data yang bersifat rahasia;
 22. Terdapat kendali aplikasi paling sedikit pada:
 - 1) Identifikasi, otentikasi, dan otorisasi;
 - 2) Antarmuka sistem;
 - 3) Keakuratan dan kelengkapan transaksi; dan
 - 4) *Logging* dan *audit trail*.
 23. Terdapat kendali infrastruktur paling sedikit pada:
 - 1) Identifikasi, otentikasi, dan otorisasi penggunaan Infrastruktur SPBE sudah dikelola;
 - 2) Di setiap sistem dilakukan instalasi perangkat lunak untuk mencegah dan mendeteksi perangkat lunak berbahaya (virus, malware, dan lain-lain);
 - 3) Pengendalian keamanan pada jaringan telah dilakukan; dan
 - 4) Dilakukan identifikasi infrastruktur yang kritis untuk dipantau.
- c. Auditor harus melakukan pemeriksaan terhadap penyediaan layanan keamanan SPBE oleh pihak eksternal paling sedikit untuk memastikan bahwa:
1. Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;
 2. Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
 3. Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan
 4. Perjanjian Kerahasiaan (*Non Disclosure Agreement*) telah ditandatangani oleh pihak eksternal.
- d. Panduan teknis dan kriteria penilaian pada audit keamanan SPBE dapat ditetapkan lebih lanjut oleh APIP, sesuai ketentuan peraturan perundang-undangan.

(1) Pembiayaan Audit TIK

- a. Pembiayaan untuk pelaksanaan Audit TIK dapat ditanggung oleh:
 1. APIP;
 2. Dinas Teknis terkait TIK; dan/atau
 3. Auditee yang mengusulkan kegiatan audit TIK.
- b. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas proses bisnis.
- c. Mekanisme penganggaran audit TIK dapat dilakukan melalui perjanjian kerja dengan pihak ketiga atau swakelola yang disesuaikan dengan ketentuan peraturan perundang-undangan.

