BUPATI KOTAWARINGIN TIMUR
PROVINSI KALIMANTAN TENGAH
PERATURAN BUPATI KOTAWARINGIN TIMUR
NOMOR 58 TAHUN 2024
TENTANG
PEDOMAN AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI KOTAWARINGIN TIMUR,

Menimbang : a. bahwa pemanfaatan teknologi informasi dan komunikasi Sistem Pemerintahan Berbasis Elektronik diharapkan dapat meningkatkan efisiensi, efektifitas, transparansi, dan akuntabilitas dalam penyelenggaraan pemerintahan dan pelayanan publik dalam rangka mewujudkan salah satu tujuan nasional untuk memajukan kesejahteraan umum sebagaimana amanat dari Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

b. bahwa dalam rangka pelaksanaan Audit Internal Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik yang terarah dan terpadu, diperlukan suatu pedoman pelaksanaan Audit Internal Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Pedoman Audit Internal Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Undonesia Tahun 1945;

2. Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat Nomor 3 Tahun 1953 tentang Pembentukan Daerah Tingkat II di Kalimantan (Lembaran-Negara Tahun 1953 Nomor 9), sebagai Undang-Undang (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 72, Tambahan Lembaran Negara Republik Indonesia Nomor 1820);

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran

Negara Republik Indonesia Nomor 4843); sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
5. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan lembaran Negara Republik Indonesia Nomor 5587); sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Nomor 5679);
6. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
7. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
10. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
11. Peraturan Daerah Kabupaten Kotawaringin Timur Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Kotawaringin Timur Tahun 2016 Nomor 9 (Lembaran Daerah Kabupaten Kotawaringin Timur Tahun 2016 Nomor 9, Tambahan Lembaran Daerah Kabupaten Kotawaringin Timur Nomor 235); sebagaimana telah diubah beberapa kali terakhir dengan Peraturan

Daerah Kabupaten Kotawaringin Timur Nomor 1 Tahun 2023 tentang Perubahan Ketiga Atas Peraturan Daerah Kabupaten Kotawaringin Timur Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Kotawaringin Timur (Lembaran Daerah Kabupaten Kotawaringin Timur Tahun 2023 Nomor 1, Tambahan Lembaran Daerah Kabupaten Kotawaringin Timur Nomor 288);

12. Peraturan Bupati Kotawaringin Timur Nomor 2 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Inspektorat Daerah Kabupaten Kotawaringin Timur (Berita Daerah Kabupaten Kotawaringin Timur Tahun 2021 Nomor 2);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG PEDOMAN AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Bupati ini, yang dimaksud dengan:

1. Daerah adalah Kabupaten Kotawaringin Timur.
2. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Kotawaringin Timur.
4. Penyelenggara Negara adalah Pejabat Negara di Lingkungan Pemerintah Daerah Kabupaten Kotawaringin Timur yang menjalankan fungsi eksekutif dan tugas pokoknya berkaitan dengan penyelenggaraan negara sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah (DPRD) dalam penyelengaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE, adalah penyelenggaraan pemerintahan yang memanfaatkan TIK untuk memberikan layanan kepada pengguna SPBE.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah teknologi untuk mengumpulkan, menyiapkan, menyimpan, mengolah, mengumumkan, menganalisis, mengambil kembali, mengirim, atau menerima data dan informasi.

8. Tata Kelola SPBE adalah kerangka yang memastikan terlaksananya pengaturan, pengarahan, dan pengendalian penerapan SPBE secara terpadu.
9. Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas.
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. Arsitektur SPBE Pemerintah Daerah adalah arsitektur SPBE yang diterapkan di Pemerintah Daerah.
13. Peta Rencana SPBE adalah dokumen yang mendeskripsikan arah dan langkah penyiapan dan pelaksanaan SPBE yang terintegrasi.
14. Peta Rencana SPBE Pemerintah Daerah adalah Peta Rencana SPBE yang diterapkan di Pemerintah Daerah.
15. Proses Bisnis adalah sekumpulan kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi masing-masing SKPD.
16. 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.
17. 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.
18. Infrastruktur SPBE Daerah adalah Infrastruktur SPBE yang diselenggarakan oleh Pemerintah Daerah.
19. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas/fungsi layanan SPBE.
20. Aplikasi Umum adalah Aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh Instansi Pusat dan/atau Pemerintah Daerah.
21. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh Instansi Pusat atau Pemerintah Daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan Instansi Pusat dan Pemerintah Daerah lain.
22. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.

23. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
24. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
25. Lembaga Pelaksana Audit TIK adalah lembaga yang melaksanakan Audit TIK.
26. Lembaga Pelaksana Audit TIK Terakreditasi dan Terdaftar adalah badan hukum yang merupakan Lembaga Pelaksana Audit TIK terakreditasi yang telah terdaftar pada lembaga yang menyelenggarakan tugas pemerintahan di bidang pengkajian dan penerapan teknologi dan/atau lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan terakreditasi berdasarkan ketentuan peraturan perundang-undangan.
27. Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
28. Audit Infrastruktur SPBE adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset infrastruktur SPBE dengan tujuan untuk menetapkan tingkat kesesuaian antara Infrastruktur SPBE dengan kriteria dan/atau standar yang telah ditetapkan.
29. Audit Aplikasi SPBE adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset Aplikasi SPBE dengan tujuan untuk menetapkan tingkat kesesuaian antara Aplikasi SPBE dengan kriteria dan/atau standar yang telah ditetapkan.
30. Audit Keamanan SPBE adalah Audit Teknologi Informasi dan Komunikasi Lingkup Keamanan SPBE.
31. Auditor adalah orang yang memiliki kompetensi, pengetahuan dan/atau keterampilan khusus dengan tugas utama melakukan evaluasi atas pengendalian sistem elektronik yang dapat dipertanggungjawabkan secara akademis maupun praktik.
32. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
33. Jaringan intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.

34. Sistem penghubung layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran layanan SPBE.
35. Pusat Data Nasional adalah sekumpulan pusat data yang digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah, dan saling terhubung.
36. Jaringan Intra Pemerintah adalah jaringan interkoneksi tertutup yang menghubungkan antar jaringan intra Instansi Pusat dan Pemerintah Daerah.
37. 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.
38. Lembaga Sertifikasi Profesi yang selanjutnya disingkat LSP adalah lembaga pelaksana sertifikasi kompetensi Auditor TIK dengan lingkup Audit Infrastruktur SPBE dan Audit Aplikasi SPBE.
39. Lembaga Pelaksana Audit SPBE yang selanjutnya disingkat LATIK SPBE adalah lembaga pelaksana audit SPBE.
40. Lembaga Audit Keamanan Informasi yang selanjutnya disebut LAKI adalah lembaga yang melaksanakan Audit Keamanan Informasi.
41. Lembaga Audit Keamanan SPBE yang selanjutnya disingkat LAKI SPBE adalah lembaga pelaksana Audit Teknologi Informasi dan Komunikasi pemerintah atau lembaga pelaksana Audit Teknologi Informasi dan Komunikasi yang terakreditasi sesuai dengan ketentuan peraturan perundang-undangan, yang melaksanakan Audit Keamanan SPBE.
42. *Auditee* adalah unit kerja yang menjadi objek dari pelaksanaan Audit Infrastruktur dan Audit Aplikasi SPBE.
43. Tim Koordinasi SPBE Pemerintah Daerah adalah tim yang dibentuk oleh Bupati yang memiliki tugas untuk mengarahkan, memantau, dan mengevaluasi pelaksanaan SPBE yang terpadu di dalam Pemerintah Daerah, serta melakukan koordinasi dengan Tim Koordinasi SPBE Nasional untuk pelaksanaan SPBE yang melibatkan lintas Pemerintah Daerah.
44. Koordinator SPBE Pemerintah Daerah adalah Sekretaris Daerah yang ditetapkan oleh Bupati sebagai Koordinator SPBE Pemerintah Daerah.
45. Pengguna SPBE adalah Pemerintah Daerah, Aparatur Sipil Negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan layanan SPBE.

Pasal 2

Standar dan tata cara pelaksanaan audit TIK SPBE digunakan sebagai pedoman bagi Pemerintah Daerah dalam melaksanakan audit internal Infrastruktur SPBE, audit internal Aplikasi SPBE dan audit internal Keamanan SPBE.

Pasal 3

Standar dan tata cara pelaksanaan audit internal Infrastruktur SPBE sebagaimana dimaksud dalam Pasal 2 tercantum dalam lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 4

Ketentuan mengenai Standar dan tata cara pelaksanaan audit internal Aplikasi SPBE sebagaimana dimaksud dalam Pasal 2 tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 5

Ketentuan mengenai Standar dan tata cara pelaksanaan audit internal Keamanan SPBE sebagaimana dimaksud dalam Pasal 2 tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 6

Ketentuan mengenai kriteria penilaian audit internal infrastruktur SPBE, audit internal Aplikasi SPBE dan audit internal Keamanan SPBE tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 7

Audit TIK SPBE di lingkungan Pemerintah Daerah terdiri atas:
a. audit internal; dan
b. audit eksternal.

Pasal 8

Pelaksanaan audit internal untuk Audit Infrastruktur SPBE, Audit Aplikasi SPBE dan Audit Keamanan SPBE dilaksanakan oleh tim audit Internal SPBE Pemerintah Daerah.

Pasal 9

Tim audit internal SPBE Pemerintah Daerah sebagaimana dimaksud dalam Pasal 8 ditetapkan dengan Keputusan Bupati.

Pasal 10

(1) Pelaksanaan audit eksternal infrastruktur SPBE dan audit eksternal Aplikasi SPBE dilaksanakan oleh Lembaga Pemerintah.
(2) Lembaga Pemerintah sebagaimana dimaksud pada ayat (1) memiliki tugas dan fungsi di bidang teknologi informasi dan komunikasi atau LATIK SPBE.
(3) Pelaksanaan audit eksternal keamanan SPBE dilaksanakan oleh Badan Siber dan Sandi Negara atau LAKI SPBE.

BAB II
KETENTUAN PENUTUP

Pasal 11

Peraturan Bupati ini mulai berlaku pada tanggal ditetapkan. Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Kotawaringin Timur.

Ditetapkan di Sampit,
pada tanggal 30 DESEMBER 2024
BUPATI KOTAWARINGIN TIMUR,

HALIKINNOR

Diundangkan di Sampit,
pada tanggal 30 DESEMBER 2024
Pj. SEKRETARIS DAERAH
KABUPATEN KOTAWARINGIN TIMUR,

SANGGUL LUMBAN GAOL

BERITA DAERAH KABUPATEN KOTAWARINGIN TIMUR TAHUN 2024 NOMOR 58

LAMPIRAN I : PERATURAN BUPATI KOTAWARINGIN TIMUR
NOMOR 58 TAHUN 2024
TENTANG PEDOMAN AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I
STANDAR PELAKSANAAN AUDIT INTERNAL INFRASTRUKTUR SPBE

Standar Pelaksanaan Audit Internal Infrastruktur SPBE 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 Internal Infrastruktur SPBE memiliki tujuan sebagai berikut :

a. menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit Internal Infrastruktur SPBE;
b. menyusun Kerangka Kerja dalam pemberian layanan jasa Audit Infrastruktur SPBE guna menambah nilai kepada yang diaudit (*Auditee*) melalui perbaikan proses dan operasionalnya; dan
c. menyusun dasar dalam melakukan evaluasi terhadap regulasi dan pelaksanaan Audit Internal Infrastruktur SPBE guna mendorong rencana perbaikan.

Standar pelaksanaan Audit Internal Infrastruktur SPBE mencakup hal-hal sebagai berikut :

1. Standar Umum;
2. Standar Pelaksanaan;
3. Standar Pelaporan; dan
4. Standar Tindak Lanjut.

1.1. Standar Umum

a. Standar Umum memberikan prinsip dasar yang mengatur Auditor Internal Infrastruktur SPBE dalam melaksanakan tugasnya sehingga pelaksanaan pekerjaan Audit Internal Infrastruktur SPBE hingga pelaporannya dapat terlaksana dengan baik dan efektif.
b. Integritas Auditor Internal Infrastruktur SPBE diwujudkan melalui sikap independen, objektif, dan menjaga kerahasiaan.
   Dalam melaksanakan tugasnya, Auditor Internal SPBE dituntut untuk menjalankan hal-hal sebagai berikut:
   1) memiliki pengetahuan (*knowledge*), keterampilan (*skill*), sikap (*attitude*), dan pengalaman (*experience*) yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung-jawabnya dalam pelaksanaan Audit;
   2) menggunakan keahlian profesionalnya dengan cermat dan seksama (*due professional care*) serta berhati-hati (*prutent*) dalam setiap penugasan;

3) senantiasa mengasah dan melatih kecermatan profesionalnya;
4) meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan; dan
5) mematuhi prosedur yang ditetapkan dan mematuhi aturan perundang-undangan.

c. Tujuan, wewenang, dan tanggung-jawab suatu aktivitas Audit Internal Infrastruktur SPBE harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam audit (*audit charter*), surat tugas, atau dokumen-dokumen yang setara. Surat tugas atau piagam audit (*audit charter*) wajib menjelaskan tujuan audit, ruang lingkup, kewenangan tim audit dan etika yang harus dipatuhi oleh tim audit internal.
d. Koordinator SPBE memberikan tugas kepada tim audit internal dalam bentuk Surat Tugas atau dapat juga berupa piagam audit (*audit charter*) sebelum Audit Internal Infrastruktur SPBE dilaksanakan.

1.2. Standar Pelaksanaan;

a. Ketua tim audit internal harus secara efektif mengelola aktivitas audit untuk menjamin agar tujuan Audit Infrastruktur SPBE tercapai.
b. Ketua tim audit internal harus memiliki hal-hal sebagai berikut:
   1) menyusun dan menetapkan rencana audit internal (internal audit plan) guna menentukan prioritas-prioritas dalam kegiatan Audit Internal Infrastruktur SPBE yang konsisten dengan tujuan audit sesuai dengan surat tugas audit atau piagam audit;
   2) menyampaikan rencana audit internal (*internal audit plan)* kepada *Auditee* untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumber daya;
   3) mengelola sumberdaya audit yang tepat, memadai, dan efektif untuk melaksanakan rencana audit internal yang telah disetujui;
   4) melakukan koordinasi dengan pimpinan LATIK SPBE untuk menjamin bahwa pelaksanaan Audit Internal Infrastruktur SPBE berjalan efektif dan efisien; dan
   5) memberi laporan yang memadai kepada pimpinan unit kerja yang diaudit mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.
c. SKPD mengajukan permintaan Audit Internal Infrastruktur SPBE untuk satu atau lebih tujuan berikut:
   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 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.

d. Pemeriksaan yang dilakukan oleh *Auditee* mencakup:
e. Dalam hal merencanakan Audite Internal Infrastruktur SPBE, Auditor harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit Internal Infrastruktur SPBE, termasuk tujuan, lingkup, waktu, dan alokasi sumber daya bagi pelaksanaan audit. Perencanaan tersebut yang dituangkan dalam rencana audit internal (*Internal Audit Plan*) dengan mempertimbangkan berbagai hal, antara lain:
   1) sistem pengendalian internal dan kepatuhan *Auditee* terhadap acuan atau *benchmark*;
   2) penetapan tujuan Audit Internal Infrastruktur SPBE;
   3) penetapan kecukupan lingkup; dan
   4) penggunaan metodologi yang tepat.
f. Dalam hal pelaksanaan audit internal Infrastruktur SPBE, Auditor Internal Infrastruktur SPBE harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai tujuan audit.
   Dalam hal melaksanakan audit internal tersebut, Auditor Internal Infrastruktur SPBE 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 internal; dan
   4) disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
g. Dalam hal komunikasi atas hasil Audit Internal Infrastruktur SPBE, Auditor Internal Infrastruktur SPBE 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. Jika komunikasi final berisi kesalahan atau penghilangan yang signifikan, ketua tim audit harus mengkomunikasikan informasi yang telah diperbaiki kepada semua pihak yang menerima komunikasi.
   Aspek pemantauan dalam aktivitas Audit Internal Infrastruktur SPBE 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.
h. Evaluasi mencakup perencanaan, pelaksanaan, dan pelaporan Audit Internal Infrastruktur SPBE.

1.3. Standar Pelaporan
   a. Laporan hasil audit dibuat dalam bentuk dokumen laporan audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas.

b. Laporan audit internal harus mencantumkan batasan atau pengecualian yang berkaitan dengan pelaksanaan audit. 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.

1.4. Standar Tindak Lanjut.

a. Pemantauan terhadap legalitas, kompetensi, dan kinerja auditor internal dilakukan melalui mekanisme registrasi dan laporan tahunan pelaksanaan audit.
b. Dalam kondisi pemantauan terhadap tindak lanjut akan dilaksanakan, ketua tim audit 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.

BAB II
TATA CARA PELAKSANAAN AUDIT INTERNAL INFRASTRUKTUR SPBE

2.1. Tata Cara Pelaksanaan Audit

Audit Internal Infrastruktur SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar 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*).

Adapun tiga kelompok tersebut meliputi hal-hal sebagai berikut:

a. penyiapan tim audit internal;
b. *quick assessment*;
c. penyiapan rencana audit internal;
d. penyepakatan rencana audit internal;
e. penyiapan protokol audit;
f. penetapan parameter acuan;
g. pertemuan pembukaan;
h. pelaksanaan lapangan;
i. pertemuan penutupan;
j. analisa data;
k. pengelolaan data;
l. penyusunan laporan;
m. *proof-read* laporan;
n. penyerahan laporan; dan
o. evaluasi aktivitas Audit Internal Infrastruktur SPBE dilakukan oleh sebuah tim audit yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut:

1) penanggung-jawab berperan melakukan monitoring dan evaluasi aktivitas audit untuk menjamin pelaksanaan audit internal sesuai dengan standar audit.
2) *Lead Auditor* bertanggung jawab merencanakan audit teknologi, melaksanakan audit di lapangan, mengendalikan data, dan melaporkan hasil audit internal. *Lead Auditor* harus mempunyai kualitas minimal setara dengan Auditor Teknologi Madya.
3) auditor internal bertugas membantu *Lead Auditor* dalam aktivitas audit teknologi. Auditor harus mempunyai kualifikasi minimal setara dengan Auditor Teknologi Muda.
4) asisten Auditor bertugas membantu Auditor dalam aktivitas audit teknologi.
5) teknisi bertugas membantu Auditor dalam pengumpulan data lapangan.
6) narasumber berperan memberi masukan yang berkaitan dengan isu, status teknologi, dan keilmuan yang relevan.

Quick Assessment dilakukan untuk mengenali objek audit dengan mengidentifikasi: isu terkini, lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, proses bisnis dari organisasi atau bagian yang diaudit.

Tim audit internal infrastruktur SPBE harus merencanakan tindakan audit 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. *deliverable*; dan
k. perkiraan jadwal pelaksanaan.

Hal-hal tersebut harus dicantumkan dalam Rencana Audit Internal (*Internal Audit Plan*). Ketua Tim Audit dan *Auditee* harus menyepakati rencana audit internal sebelum tahap pelaksanaan audit.

Dalam pelaksanaan kegiatan audit, tim Audit Internal Infrastruktur SPBE harus:

(1) menyusun protokol audit yang berisi detail instrument audit, antara lain:
   a. daftar data, pertanyaan, dan pengujian; dan
   b. formulir untuk mencatat data, jawaban, hasil observasi, dan hasil pengujian.
(2) menetapkan parameter acuan untuk setiap kriteria yang diperlukan untuk memberikan suatu acuan pembanding;
(3) melakukan pertemuan pembukaan dengan *Auditee*;
(4) melaksanakan audit lapangan, melalui:
   a. penelaahan dokumen;
   b. wawancara;

c. observasi lapangan;
d. pengujian; dan
e. verifikasi bukti.

(5) melakukan pertemuan penutupan dengan *Auditee*;
(6) melakukan analisis bukti; dan
(7) mengelola data.

Data status teknologi SPBE dikumpulkan secara objektif berdasarkan fakta yang ada pada *Auditee*. Deskripsi data dan informasi yang dikumpulkan mengikuti kriteria penilaian yang sudah dikeluarkan dalam angka II dari Lampiran IV dan ditetapkan tersendiri oleh Koordinator SPBE.

Temuan Audit Internal Infrastruktur SPBE merupakan keadaan dimana fakta status aset teknologi SPBE *Auditee* tidak sesuai dengan persyaratan infrastruktur SPBE. Auditor internal dapat mengurangi atau menambahkan lingkup data sebagaimana tercantum dalam angka III dari Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini sepanjang relevan dengan objek dan rencana penggunaan hasil audit internal sesuai kebutuhan *Auditee*.

Pemantauan memberikan informasi untuk suatu kegiatan audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam pelaksanaan audit.

Tim pengawas mutu dapat berasal dari pihak eksternal.

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. Evaluasi dilakukan oleh tim pengawas mutu setelah aktivitas audit selesai.

Tim pengawas mutu menyampaikan hasil evaluasi audit kepada Bupati melalui Koordinator SPBE. Koordinator SPBE menetapkan kebijakan tindak lanjut berdasarkan hasil evaluasi audit internal.

2.2. Tata Cara Pelaporan Audit

Laporan audit internal disampaikan oleh ketua tim audit internal kepada Bupati melalui Koordinator SPBE. Laporan mencakup latar belakang, tujuan, lingkup, pendekatan audit, kriteria dan acuan, metode pengumpulan data, metode analisis, hasil analisis, temuan dan kesimpulan, dan rekomendasi.

Pada setiap halaman dokumen laporan audit diberi identifikasi (nomor dokumen) yang menggambarkan sekurang-kurangnya: tahun pelaksanaan audit internal, nomor urut atau nomor seri dokumen, domain Aplikasi atau Infrastruktur SPBE, *Auditee*, dan kode pengendalian distribusi salinan dokumen. Draf laporan direviu oleh ketua tim audit internal untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit.

Laporan Audit disahkan oleh Bupati, diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli. Laporan Audit Internal didistribusikan kepada Bupati.

Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh Bupati kepada Badan Pengkajian dan Penerapan Teknologi (BPPT) satu kali dalam satu tahun dengan format sebagai berikut:

FORMAT LAPORAN PERIODIK AUDIT INTERNAL INFRASTRUKTUR SPBE

A. Identitas Tim Auditor Internal
Nama Tim Auditor Internal (isi nama Tim Pelaksana Audit Internal)
Periode pelaporan (isi periode Audit)

B. Penanggungjawab Penyelenggaraan Audit
Nama (isi nama lengkap)
Jabatan (isi jabatan resmi)
NIP (isi nomor induk pegawai)
Kontak (isi nomor telepon dan alamat surat elektronik ybs)

C. Penyelenggaraan Audit
Judul Audit TIK (isi judul)
Tanggal Laporan Audit (isi tanggal)
Jenis Audit (isi jenis audit)
Lingkup Audit (isi lingkup audit)
Ringkasan Hasil Audit Ringkasan Temuan (parameter)
Ringkasan Rekomendasi (parameter) (temuan 1)
Jenis dan narasi (rekomendasi 1)
Narasi singkat dan tenggal waktu (temuan 2) (rekomendasi 2)

D. Tindak Lanjut Audit, Informasi Tindak Lanjut Audit Rekomendasi
#1 Tenggat waktu Tindak Lanjut
#1 Rekomendasi
#2 Tenggat waktu Tindak Lanjut
#2 Rekomendasi
#3 Tenggal Waktu Tindak Lanjut
#3 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.

Laporan pelaksanaan audit internal dibuat oleh Badan Pengkajian dan Penerapan Teknologi (BPPT) berdasarkan hasil pelaporan oleh Bupati kepada tim koordinasi SPBE nasional dan lembaga lain sesuai ketentuan peraturan perundang-undangan.

2.3. Tata Cara Tindak Lanjut Audit

Kesepakatan proses pemantauan yang disepakati oleh Tim Auditor dan *Auditee* yang sekurang-kurangnya meliputi: lingkup, objek, jangka waktu, beban pembiayaan, dan penanggungjawab.

Pemantauan dapat dilakukan oleh Tim Auditor Internal atau Auditor lain yang disepakati. Konfirmasi terhadap hasil audit dilakukan paling banyak tiga kali.

Tindak lanjut perbaikan dari *Auditee* perlu dievaluasi oleh Auditor. Evaluasi dilakukan untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi *Auditee*.

2.4. Tata Cara Pembiayaan Audit

Pembiayaan untuk pelaksanaan Audit Internal ditanggung dibebankan pada anggaran Daerah didasarkan pada cakupan area audit sesuai dengan kompleksitas proses bisnis sesuai ketentuan peraturan perundang-undangan.

BAB III
PANDUAN TEKNIS AUDIT INTERNAL INFRASTRUKTUR SPBE

3.1. Panduan Teknis Umum Audit Infrastruktur SPBE

Ruang lingkup Panduan Teknis Umum Audit Infrastruktur SPBE adalah sebagai berikut:

a. Tata Kelola Infrastruktur SPBE;
b. Manajemen Infrastruktur SPBE; dan
c. Fungsionalitas dan kinerja infrastruktur SPBE.

Ruang lingkup panduan audit internal tata kelola infrastruktur SPBE mencakup aktivitas:

a. Evaluasi;
b. Pengarahan; dan
c. Pemantauan.

Ruang lingkup panduan audit internal manajemen infrastruktur SPBE terdiri atas tahapan:

a. Perencanaan;
b. Pengambangan;
c. Pengoperasian; dan
d. Pemantauan.

Audit internal manajemen infrastruktur mencakup aktivitas:

a. Manajemen sistem pengendalian internal;
b. Manajemen risiko;
c. Manajemen aset;
d. Manajemen pengetahuan;
e. Manajemen sumber daya manusia;
f. Manajemen layanan;
g. Manajemen perubahan; dan
h. Manajemen data.

Ruang lingkup panduan fungsionalitas dan kinerja infrastruktur SPBE terdiri atas tahapan:

a. Perencanaan;
b. Pengembangan;
c. Pengoperasian; dan
d. Pemeliharaan.

Hal teknis yang diaudit difokuskan pada Fungsionalitas dan Kinerja Infrastruktur SPBE.

3.2. Panduan Teknis Audit Internal Jaringan Intra Pemerintah Daerah

Panduan teknis audit internal Jaringan Intra Pemerintah Daerah dimaksudkan sebagai panduan dalam pelaksanaan audit internal Jaringan Intra Pemerintah di Pemerintah Kabupaten Kotawaringin Timur.

Audit teknis Jaringan Intra Pemerintah di Pemerintah Daerah mencakup fungsionalitas dan kinerja. Lingkup panduan teknis audit internal Jaringan Pemerintah di Kabupaten Kotawaringin Timur terdiri atas:

a. Perencanaan Jaringan Intra Pemerintah;
b. Pengembangan Jaringan Intra Pemerintah;
c. Pengoperasian Jaringan Intra Pemerintah; dan
d. Pemeliharaan Jaringan Intra Pemerintah.

Jaringan Intra Pemerintah Daerah direncanakan dengan mengacu kepada Arsitektur SPBE Nasional, Arsitektur SPBE Pemerintah Daerah, Peta Rencana SPBE Nasional, dan Peta Rencana SPBE.

Perencanaan Jaringan Intra Pemerintah Daerah disusun berdasarkan persyaratan Jaringan Intra Pemerintah dengan mempertimbangkan kebutuhan dan infrastruktur SPBE Nasional mencakup kebutuhan bisnis, kebutuhan jaringan, dan rancangan jaringan.

Jaringan intra pemerintah dapat dikembangkan oleh tim internal Pemerintah Daerah atau dari pihak ketiga dengan mengacu kepada deskripsi dalam rancangan. Konfigurasi jaringan SPBE dapat dikustomisasi dan dilengkapi dengan dokumentasi yang memadai.

Uji coba terhadap jaringan intra pemerintah di Daerah harus terdokumentasi dalam suatu rencana pengujian (*test plan*), rancangan pengujian (*test design*), prosedur pengujian (*test procedures*), dan laporan pengujian (*test report*).

Jaringan Intra Pemerintah Daerah dilengkapi dengan dokumen penggunaan Jaringan Intra Pemerintah baik untuk operator maupun administrator. Dokumentasi tersebut mencakup:

a. penggunaan perangkat Jaringan Intra Pemerintah di Daerah antara lain: cara instalasi, akses terhadap perangkat, operasi terhadap perangkat;
b. prosedur dan tutorial; dan
c. gangguan dan penanganannya.

Pemeliharaan terhadap Jaringan Intra Pemerintah di Daerah didokumentasikan dalam suatu dokumen yang mencakup pemeliharaan jaringan dan manajemen konfigurasi jaringan.

3.3. Panduan Teknis Audit Internal Sistem Penghubung Layanan Pemerintah

Panduan teknis audit Sistem Penghubung Layanan Pemerintah di Daerah dimaksudkan sebagai panduan dalam pelaksanaan audit infrastruktur SPBE.

Audit teknis Sistem Penghubung Layanan Pemerintah di Daerah mencakup fungsionalitas dan kinerja lingkup panduan teknis audit Sistem Penghubung Layanan terdiri atas:

a. Perencanaan Sistem Penghubung Layanan Pemerintah Daerah;

b. Pengembangan Sistem Penghubung Layanan Pemerintah;
c. Pengoperasian Sistem Penghubung Layanan Pemerintah; dan
d. Pemeliharaan Sistem Penghubung Layanan Pemerintah.

Sistem Penghubung Layanan Pemerintah direncanakan dengan mengacu kepada arsitektur SPBE nasional, arsitektur SPBE Pemerintah Daerah, peta rencana SPBE nasional, dan peta rencana SPBE Pemerintah Daerah.

Perencanaan Sistem Penghubung Layanan Pemerintah di Daerah mencakup prinsip, kebijakan, dan organisasi.

Sistem Penghubung Layanan Pemerintah di Daerah dapat dikembangkan oleh tim internal daerah atau pihak ketiga dengan mengacu kepada deskripsi dalam rancangan.

Pengembangan Sistem Penghubung Layanan Pemerintah di Daerah mencakup implementasi, pengujian, dan instalasi.

Uji coba terhadap Sistem Penghubung Layanan Pemerintah di Daerah harus terdokumentasi dalam suatu rencana pengujian (*test plan*), rancangan pengujian (*test design*), prosedur pengujian (*test Procedures*), dan laporan pengujian (*test report*).

Sistem Penghubung Layanan Pemerintah dilengkapi dengan dokumentasi penggunaan Sistem Penghubung Layanan Pemerintah di Daerah baik untuk operator maupun administrator. Dokumentasi tersebut mencakup penyelenggaraan dan mekanisme kerja. Pemeliharaan terhadap jaringan intra pemerintah daerah didokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:
a. lingkup pemeliharaan;
b. alokasi sumber daya; dan
c. pencatatan kinerja.

Kriteria penilaian audit infrastruktur SPBE yang terdiri atas Tata Kelola dan Manajemen, Pusat Data, Jaringan Intra Pemerintah, dan Sistem Penghubung Layanan Pemerintah Daerah tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

BAB IV
AUDITOR INFRASTRUKTUR SPBE

Auditor Infrastruktur SPBE merupakan Auditor Teknologi yang memiliki kemampuan teknis di bidang Infrastruktur TIK.

Ketua Tim Audit wajib memiliki sertifikat kompetensi Auditor. Sertifikasi kompetensi Auditor teknologi dilaksanakan oleh Lembaga Sertifikasi Profesi (LSP) bidang kompetensi Auditor teknologi atau LSP yang mendapat pengakuan dari Badan Riset dan Inovasi Nasional (BRIN).

Calon Auditor SPBE mengajukan permohonan Surat Tanda Registrasi sebagai Auditor SPBE kepada Kepala Badan Riset dan Inovasi Nasional (BRIN) dengan menggunakan format sebagaimana yang dikeluarkan oleh Badan Riset dan Inovasi Nasional (BRIN). Permohonan pendaftaran dilengkapi dengan dokumen:
a. Surat permohonan;

b. Sertifikat kompetensi di bidang Audit Infrastruktur TIK yang mendapat pengakuan dari Badan Riset dan Inovasi Nasional (BRIN). Auditor SPBE yang telah memperoleh Surat Tanda Registrasi sebagaimana dimaksud pada ayat (4) dinyatakan dalam Daftar Auditor SPBE. Surat Tanda Registrasi Auditor SPBE dinyatakan tidak berlaku apabila:
   1) melanggar kode etik;
   2) meninggal dunia;
   3) habis masa berlaku Surat Tanda Registrasi; dan
   4) mengundurkan diri.

   Masa berlaku Surat Tanda Registrasi dapat diperpanjang dengan cara melengkapi kembali dokumen pendaftaran.

4.1. Prosedur Pendaftaran Auditor Infrastruktur SPBE Prosedur Pendaftaran Auditor Infrastruktur SPBE disesuaikan dengan prosedur pendaftaran auditor di Badan Riset dan Inovasi Nasional (BRIN).

4.2. Format Permohonan Surat Tanda Registrasi Auditor Infrastruktur SPBE disesuaikan dengan yang dikeluarkan oleh Badan Riset dan Inovasi Nasional (BRIN).

FORMAT PERMOHONAN
SURAT TANDA REGISTRASI AUDITOR INFRASTRUKTUR SPBE

Kepada Yth.
Kepala Badan Pengkajian dan Penerapan Teknologi

Di -
Jakarta

Yang bertanda tangan di bawah ini :

Nama	: [Nama]
NIK	: [Nomor KTP]
Nomor Telepon	: [Nomor telepon 1, nomor telepon 2, dsb.]
E-mail	: [Alamat E-mail 1, Alamat E-mail 2, dsb.]
Alamat	: [Tulis alamat lengkap sesuai domisili]

Dengan ini mengajukan permohonan/perpanjangan*) Surat Tanda Registrasi AUDITOR Infrastruktur SPBE. Bersama ini kami sampaikan pula kelengkapan dokumen dalam bentuk *hardcopy* dan/*softcopy*.
Kami bertanggung jawab atas kebenaran dari dokumen dan/atau data-data yang dipersyaratkan.

[Nama Kota, Tanggal Bulan Tahun]

Pemohon

[Nama]

BUPATI KOTAWARINGIN TIMUR,

HALIKINNOR

LAMPIRAN II : PERATURAN BUPATI KOTAWARINGIN TIMUR
NOMOR 58 TAHUN 2024
TENTANG PEDOMAN AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I
STANDAR PELAKSANAAN AUDIT INTERNAL APLIKASI SPBE

Standar Audit Internal Aplikasi SPBE merupakan batasan minimal bagi Regulator dan Auditor guna membantu dalam proses pendaftaran Auditor terakreditasi, pelaksanaan Audit serta prosedur yang harus dilaksanakan atau diterapkan dalam rangka pencapaian tujuan Audit.

Tujuan dari Standar Audit Internal Aplikasi SPBE adalah sebagai berikut:

a. menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit Aplikasi SPBE;
b. menyusun Kerangka Kerja regulasi Audit Internal Aplikasi SPBE dalam proses pendaftaran Auditor dan Lembaga Audit Terakreditasi;
c. menyusun Kerangka Kerja dalam pemberian layanan jasa Audit Aplikasi SPBE, guna menambah nilai kepada *Auditee* melalui perbaikan proses dan operasionalnya; dan
d. menyusun dasar dalam melakukan evaluasi terhadap regulasi dan pelaksanaan Audit Internal Aplikasi SPBE guna mendorong rencana perbaikan.

Standar Audit Internal Aplikasi mencakup hal-hal sebagai berikut :

a. Standar Umum;
b. Standar Pelaksanaan;
c. Standar Pelaporan; dan
d. Standar Tindak Lanjut.

1.1. Standar Umum

a. Standar Umum memberikan prinsip dasar untuk mengatur Auditor Internal Aplikasi SPBE dalam melaksanakan tugasnya, dan mengatur pendaftaran Auditor sehingga pelaksanaan pekerjaan Audit Internal Aplikasi SPBE hingga pelaporannya dapat terlaksana dengan baik dan efektif.
b. Integritas Auditor Internal Aplikasi SPBE dan pelaksana pendaftaran diwujudkan melalui sikap independen, objektif, dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor Internal Aplikasi SPBE dituntut untuk menjalankan hal-hal sebagai berikut:
   1) memiliki pengetahuan (*knowledge*), keterampilan (*skill*), sikap (*attitude*), dan pengalaman (*experience*) yang sesuai dengan standar kompetensi Auditor, guna memenuhi tanggung jawabnya dalam pelaksanaan audit;

2) menggunakan keahlian profesionalnya dengan cermat dan seksama (*due professional care*) serta berhati-hati (*prudent*) dalam setiap penugasan;
3) senantiasa mengasah dan melatih kecermatan profesionalnya;
4) meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan;
5) mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
6) memiliki pengetahuan (*knowledge*), keterampilan (*skill*), sikap (*attitude*), dan pengalaman (*experience*) yang sesuai guna memenuhi tanggung jawabnya dalam pelaksanaan audit.

c. Tujuan, wewenang, dan tanggung jawab suatu aktivitas Audit Internal Aplikasi SPBE harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam audit (*audit charter*), surat tugas, atau dokumen-dokumen yang setara.
d. Bupati memberikan tugas kepada tim audit internal dalam bentuk Surat Tugas atau dapat juga berupa piagam audit (*audit charter*) sebelum Audit Internal Aplikasi SPBE dilaksanakan.

1.2. Standar Pelaksanaan

a. Ketua tim audit internal harus secara efektif mengelola aktivitas audit untuk menjamin agar tujuan audit internal Aplikasi SPBE tercapai. Ketua tim audit internal harus melakukan hal-hal sebagai berikut:
   1) menyusun dan menetapkan rencana audit internal (*internal audit plan*) guna menentukan prioritas-prioritas dalam kegiatan Audit Internal Aplikasi SPBE, yang konsisten dengan tujuan audit sesuai dengan piagam audit (*audit charter*);
   2) menyampaikan rencana audit internal (*internal audit plan*) kepada *Auditee* untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumber daya;
   3) mengelola sumberdaya audit internal yang tepat, memadai dan efektif untuk melaksanakan rencana audit internal yang telah disetujui; dan
   4) memberi laporan yang memadai kepada Bupati mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit internal.
b. Daerah wajib melaksanakan Aktivitas Audit Internal Aplikasi SPBE untuk tujuan sebagai berikut:
   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 daya saing/kemampuan teknologi yang dimiliki, 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.

c. Pemeriksaan yang dilakukan mencakup:
   1) penerapan tata kelola dan manajemen Aplikasi SPBE;
   2) fungsionalitas dan kinerja Aplikasi SPBE; dan
   3) tingkat kepatuhan terhadap regulasi.
d. Dalam hal merencanakan audit internal Aplikasi SPBE, Auditor internal harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan audit internal Aplikasi SPBE, termasuk tujuan, lingkup, waktu, dan alokasi sumber daya bagi pelaksanaan audit.
e. Perencanaan tersebut yang dituangkan dalam Rencana Audit (*Audit Plan*) dengan mempertimbangkan berbagai hal, antara lain:
   1) sistem pengendalian internal dan kepatuhan *Auditee* terhadap acuan atau *benchmark*;
   2) penetapan tujuan audit internal aplikasi SPBE;
   3) penetapan kecukupan lingkup; dan
   4) penggunaan metodologi yang tepat.
f. Dalam hal pelaksanaan audit internal Aplikasi SPBE, Auditor Aplikasi SPBE harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai tujuan audit. Dalam melaksanakan audit tersebut, Audit Internal Aplikasi SPBE harus:
   1) memperoleh bukti-bukti audit internal yang cukup, handal dan relevan untuk mendukung penilaian dan kesimpulan;
   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 internal; dan
   4) disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
g. Dalam hal komunikasi atas hasil audit internal Aplikasi SPBE, Auditor Intenral Aplikasi SPBE 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.
h. Jika komunikasi final berisi kesalahan atau penghilangan yang signifikan, ketua tim audit internal harus mengkomunikasikan informasi yang telah diperbaiki kepada semua pihak yang menerima komunikasi.
   Aspek pemantauan dalam aktivitas Audit Internal Aplikasi SPBE 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.
i. Evaluasi mencakup perencanaan, pelaksanaan, dan pelaporan audit internal Aplikasi SPBE. Bupati menetapkan kebijakan tindak lanjut berdasarkan hasil evaluasi audit.

1.3. Standar Pelaporan

a. Laporan hasil audit internal dibuat oleh Tim Auditor dalam bentuk Dokumen Laporan Audit Internal dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas.
b. Laporan Audit Internal harus mencantumkan batasan atau pengecualian yang berkaitan dengan pelaksanaan Audit Internal.
Auditor Internal 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.

1.4. Standar Tindak Lanjut

Dalam kondisi pemantauan terhadap tindak-lanjut akan dilaksanakan, ketua tim audit internal harus menetapkan sebuah sistem pemantauan terhadap tindak lanjut temuan, kesimpulan, dan rekomendasi audit internal oleh *Auditee*, mencakup cara berkomunikasi dengan *Auditee*, prosedur pemantauan, dan laporan status temuan.

BAB II
TATA CARA PELAKSANAAN AUDIT INTERNAL APLIKASI SPBE

2.1. Tata Cara Pelaksanaan Audit

Audit Internal Aplikasi SPBE dilakukan Tim Auditor Internal berdasarkan permintaan *Auditee* atau penugasan Bupati. Audit Aplikasi SPBE dilaksanakan mengikuti tata cara audit yang secara garis besar 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*)

Adapun tiga kelompok tersebut meliputi hal-hal sebagai berikut:

a. penyiapan tim audit;
b. *quick assessment*;
c. penyiapan rencana audit;
d. penyepakatan rencana audit;
e. penyiapan protokol audit;
f. penetapan parameter acuan;
g. pertemuan pembukaan;
h. pelaksanaan lapangan;
i. pertemuan penutupan;
j. analisa data;
k. pengelolaan data;
l. penyusunan laporan;
m. *proof read* laporan;
n. penyerahan laporan; dan
o. evaluasi aktivitas.

Audit Aplikasi SPBE dilakukan oleh sebuah tim audit yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut :

a. penanggungjawab berperan melakukan pemantauan dan evaluasi aktivitas audit untuk menjamin pelaksanaan audit sesuai dengan standar audit. Penanggung jawab harus memiliki kualifikasi Auditor Teknologi Utama atau yang setara;
b. *lead auditor* bertanggung jawab merencanakan audit teknologi, melaksanakan audit di lapangan, mengendalikan data, dan melaporkan hasil audit teknologi. *Lead Auditor* harus mempunyai kualifikasi minimal setara dengan Auditor Teknologi Madya;
c. auditor, bertugas membantu *Lead Auditor* dalam aktivitas audit teknologi. Auditor harus mempunyai kualifikasi minimal setara dengan Auditor Teknologi Muda;
d. asisten Auditor bertugas membantu Auditor dalam aktivitas audit teknologi;
e. teknisi, bertugas membantu Auditor dalam pengumpulan data lapangan; dan
f. narasumber, berperan memberi masukan yang berkaitan dengan isu, status teknologi, dan keilmuan yang relevan.

Quick Assessment dilakukan untuk mengenali objek audit dengan mengidentifikasi: *Current issues*, lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, proses bisnis dari organisasi, atau bagian yang diaudit.

Tim Audit Aplikasi SPBE harus merencanakan tindakan audit 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.

Hal-hal tersebut harus dicantumkan dalam Rencana Audit (*Audit Plan*).
Ketua tim audit dan *Auditee* harus menyepakati rencana audit sebelum tahap pelaksanaan audit.
Dalam pelaksanaan kegiatan audit, Tim Audit Aplikasi SPBE harus:

(1) Menyusun protokol audit yang berisi detail instrumen audit, antara lain:
    a. daftar data, pertanyaan, dan pengujian; dan

b. formulir untuk mencatat data, jawaban, hasil observasi, dan hasil pengujian.

(2) Menetapkan parameter acuan untuk setiap kriteria diperlukan untuk memberikan suatu acuan pembanding.

(3) Melakukan Pertemuan Pembukaan dengan *Auditee.*

(4) Melaksanakan audit lapangan melalui :

a. penelaahan dokumen;
b. wawancara;
c. observasi lapangan;
d. pengujian; dan
e. verifikasi bukti.

(5) Melakukan Pertemuan Penutupan dengan *Auditee.*

(6) Melakukan analisa bukti.

(7) Mengelola data.

Data status teknologi SPBE dikumpulkan secara objektif berdasarkan fakta yang ada pada *Auditee.* Deskripsi data dan informasi yang dikumpulkan mengikuti kriteria penilaian yang sudah dikeluarkan dalam BAB III dari Lampiran IV dan bagian yang tidak terpisahkan dari Peraturan Bupati ini.

Temuan Audit Aplikasi SPBE merupakan keadaan dimana fakta status aset teknologi SPBE *Auditee* tidak sesuai dengan persyaratan teknis Aplikasi SPBE.

Auditor dapat mengurangi atau menambahkan lingkup data sebagaimana tercantum dalam BAB III Lampiran IV Peraturan ini, sepanjang relevan dengan objek dan rencana penggunaan hasil audit sesuai kebutuhan *Auditee.*

Pemantauan memberikan informasi untuk suatu kegiatan audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam melaksanakan audit.

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.

2.2. Tata Cara Pelaporan Audit Internal

Laporan audit disampaikan oleh ketua tim audit kepada Bupati. Laporan mencakup latar belakang, tujuan, lingkup, pendekatan audit, kriteria dan acuan, metode pengumpulan data, metode analisis, hasil analisis, temuan dan kesimpulan, dan rekomendasi.

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.

Draft laporan direviu oleh ketua tim audit untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit. Laporan Audit disahkan oleh Bupati. Laporan Audit diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli.

Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh Koordinator SPBE kepada Bupati satu kali dalam satu tahun dengan format sebagai berikut :

FORMAT LAPORAN PERIODIK AUDIT APLIKASI SPBE

A. Identifikasi LATIK, Nama LATIK (isi nama Lembaga Pelaksana Audit) Periode Pelaporan (isi periode pelaporan)
B. Penanggung-jawab Penyelenggaraan Audit, Nama (isi nama lengkap), Jabatan (isi jabatan resmi), NIP (isi Nomor induk pegawai), Kontak (isi nomor telepon dan surel ybs).
C. Penyelenggaraan Audit, Judul Audit TIK (isi judul) Tanggal Laporan Audit (isi tanggal) Jenis Audit (isi jenis audit) Lingkup Audit (isi lingkup audit) Ringkasan Hasil Audit Ringkasan Temuan (parameter) Ringkasan Rekomendasi (parameter) (temuan 1) jenis dan narasi (rekomendasi 1) narasi singkat dan tenggat waktu (temuan 2) (rekomendasi 2).
D. Tindak Lanjut Audit Informasi Tindak Lanjut Audit Rekomendasi
   #1 Tenggal waktu Tindak Lanjut
   #1 Rekomendasi
   #2 Tenggal waktu Tindak Lanjut
   #2 Rekomendasi
   #3 Tenggat waktu Tindak Lanjut
   #3 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.

Laporan pelaksanaan audit dibuat oleh Badan Pengkajian dan Penerapan Teknologi (BPPT) berdasarkan hasil pelaporan oleh Bupati disampaikan kepada tim koordinasi SPBE nasional dan lembaga lain sesuai ketentuan peraturan perundang-undangan.

2.3. Tata Cara Tindak Lanjut Audit Internal

Kesepakatan proses pemantauan dilakukan dalam bentuk observasi pada *Auditee* pada waktu yang disepakati oleh Tim Auditor dan *Auditee* yang sekurang-kurangnya meliputi: lingkup, objek, jangka waktu, beban pembiayaan, dan penanggung-jawab. Pemantauan dapat dilakukan oleh Tim Auditor.

Konfirmasi terhadap hasil audit dilakukan paling banyak tiga kali.

Pemantauan dilakukan dalam bentuk observasi pada *Auditee* pada waktu yang disepakati oleh tim koordinasi SPBE. Tindak lanjut perbaikan dari *Auditee* perlu dievaluasi oleh Auditor.

Evaluasi dilakukan untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi *Auditee.*

2.4. Tata Cara Pembiayaan Audit Internal

Pembiayaan untuk pelaksanaan Audit ditanggung oleh Pemerintah Daerah. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas proses bisnis. Pembiayaan dan mekanisme pelaksanaannya dapat dilakukan melalui kontrak atau swakelola sesuai ketentuan perundang-undangan.

BAB III
PANDUAN TEKNIS AUDIT INTERNAL APLIKASI SPBE

3.1. Panduan Teknis Umum Audit Internal Aplikasi SPBE

Panduan teknis Audit Internal Aplikasi SPBE dimaksudkan sebagai acuan dalam menetapkan lingkup area audit internal aplikasi, kriteria audit, dan penilaian status teknologi aplikasi SPBE.

Ruang lingkup panduan audit internal tata kelola Aplikasi SPBE mencakup aktivitas :

a. Evaluasi Tata Kelola;
b. Pengarahan Tata Kelola; dan
c. Pemantauan Tata Kelola.

Audit Manajemen Aplikasi mencakup aktivitas:

a. Manajemen Sistem Pengendalian Internal;
b. Manajemen Risiko;
c. Manajemen Aset;
d. Manajemen Pengetahuan;
e. Manajemen Sumber Daya Manusia (SDM);
f. Manajemen Layanan;
g. Manajemen Perubahan; dan
h. Manajemen Data.

Ruang lingkup Panduan Fungsionalitas dan Kinerja Aplikasi SPBE terdiri atas tahapan:

a. Perencanaan Aplikasi;
b. Pengembanan Aplikasi;
c. Pengoperasian Aplikasi; dan
d. Pemeliharaan Aplikasi.

Perencanaan Aplikasi disusun dalam suatu dokumen menggunakan basis spesifikasi yang mencakup unsur:

a. kemampuan Aplikasi; dan
b. persyaratan Proses Bisnis di Daerah.

Kemampuan aplikasi mengacu pada:

a. arsitektur SPBE secara berjenjang; dan
b. persyaratan bisnis organisasi.

Arsitektur SPBE terdiri atas arsitektur SPBE Nasional dan arsitektur SPBE Pemerintah Daerah. Persyaratan proses bisnis *Auditee* dirumuskan dengan mempertimbangkan kebutuhan, peluang, dan proses bisnis. Persyaratan tersebut diterjemahkan ke dalam persyaratan aplikasi yang mencakup kebutuhan fungsi, antar muka, data, kinerja, dan batasan rancangan.

Rancangan aplikasi disusun berdasarkan persyaratan aplikasi serta memperhatikan kesesuaiannya terhadap ketentuan perundangan dan integrasi data. Rancangan tersebut beserta penjelasannya didokumentasikan sebagai Dokumen Deskripsi Rancangan Aplikasi.

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. Kode sumber (*source code*) aplikasi menggunakan *open source*, dapat dikustomisasi, dan dilengkapi dengan dokumentasi yang memadai. Pengembangan aplikasi SPBE harus disertai dengan uji coba fungsionalitasnya. Pembangunan aplikasi (*system build procedures*) yang dilengkapi dengan panduan instalasi aplikasi untuk menerapkan aplikasi di lingkungan perundangan yang berlaku. Pengembangan aplikasi harus dilengkapi dengan dokumentasi penggunaan aplikasi dan tanggung jawab data pengguna. Penggunaan aplikasi mencakup pengguna dengan klasifikasi *end-sert*, dan administrator.

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*).

Kinerja perngoperasian aplikasi dapat dievaluasi dari fungsi komponen perangkat lunak sistem elektronik yang digunakan untuk menjalankan SPBE.

Kinerja sistem elektronik untuk mendukung fungsi Pemerintah Daerah 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 bisnis *Auditee*.

Pemeliharaan terhadap aplikasi didokumentasikan dalam suatu dokumen pemeliharaan yang mencakup:

a. lingkup pemeliharaan;
b. alokasi sumber daya;
c. pencatatan kinerja; dan
d. urutan/rangkaian proses pemeliharaan.

Perubahan terhadap aplikasi didokumentasikan dalam suatu dokumen *Offware Configuration Management* yang mencakup:

a. lingkup konfigurasi;
b. aktivitas dan manajemen konfigurasi;
c. sumber daya konfigurasi; dan
d. penjadwalan manajemen konfigurasi.

Kriteria penilaian audit internal aplikasi SPBE tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

BAB IV
AUDITOR APLIKASI SPBE

Auditor aplikasi SPBE merupakan Auditor Teknologi yang memiliki kemampuan teknis di bidang Aplikasi TIK.

Ketua tim audit internal wajib memiliki sertifikat kompetensi Auditor.

Sertifikat kompetensi Auditor Teknologi sebagaimana dimaksud dalam ayat (2) dilaksanakan oleh Lembaga Sertifikasi Profesi (LSP) bidang Kompetensi Auditor Teknologi atau LSP yang mendapat pengakuan dari Badan Riset dan Inovasi Nasional (BRIN).

Calon Auditor SPBE mengajukan permohonan Surat Tanda Registrasi sebagai Auditor SPBE kepada Kepala Badan Riset dan Inovasi Nasional (BRIN) dengan menggunakan format sesuai yang dikeluarkan oleh Badan Riset dan Inovasi Nasional (BRIN).

Permohonan pendaftaran kepada Kepala Badan Riset dan Inovasi Nasional (BRIN) dilengkapi dengan dokumen:

a. surat permohonan; dan
b. sertifikat kompetensi di bidang Audit Aplikasi TIK yang mendapat pengakuan dari Badan.

Kepala Badan Riset dan Inovasi Nasional (BRIN) menetapkan Surat Tanda Registrasi Auditor SPBE paling lambat 14 (empat belas) hari kerja setelah permohonan dinyatakan valid dan lengkap. Surat Tanda Registrasi berlaku sesuai dengan masa berlaku sertifikat kompetensi Auditor Aplikasi SPBE. Auditor SPBE yang telah memperoleh Surat Tanda Registrasi sebagaimana dimaksud pada ayat (4) dinyatakan dalam Daftar Auditor SPBE. Surat Tanda Registrasi Auditor SPBE dinyatakan tidak berlaku apabila:

a. melanggar kode etik;
b. meninggal dunia;
c. habis masa berlaku Surat Tanda Registrasi; dan
d. mengundurkan diri.

Masa berlaku Surat Tanda Registrasi dapat diperpanjang dengan cara melengkapi kembali dokumen pendaftaran.

4.1. Prosedur Pendafataran Auditor Aplikasi SPBE

Prosedur Pendaftara Auditor Aplikasi SPBE adalah sebagai berikut:

(1) Prosedur Pendaftaran Audit Aplikasi SPBE untuk Auditor SPBE tersertifikasi dilakukan dengan mengikuti tahapan berikut:
   a. Auditor SPBE melengkapi persyaratan pendaftaran secara online melalui situs yang ditetapkan. Auditor SPBE melakukan pengisian beberapa formulir yang diperlukan dan melampirkan dokumen elektronik yang disyaratkan.
   b. Dokumen elektronik yang diserahkan dapat bertanda-tangan elektronik untuk memudahkan proses pendaftara.
   c. Badan Riset dan Inovasi Nasional (BRIN) akan menerbitkan izin Auditor Aplikasi SPBE untuk melakukan audit Aplikasi SPBE jika persyaratannya lengkap dan valid.

(2) Dalam hal kesiapan pendaftaran secara *online* dan/atau kesiapan penerapan penggunaan tanda-tangan elektronik belum memadai, maka proses pendaftaran dapat dilakukan secara manual.

4.2. format Permohonan Surat Tanda Registrasi Auditor Aplikasi SPBE

Kepada Yth.
Kepala Badan Pengkajian dan Penerapan Teknologi/Badan Riset dan Inovasi Nasional
di -
Jakarta

Yang bertanda-tangan di bawah ini:

Nama	: [Nama]
NIK	: [Nomor KTP]
Nomor Telepon	: [Nomor telepon 1, nomor telepon 2, dsb]
E-mail	: [Alamat E-mail 1, Alamat E-mail 2, dsb]
Alamat	: [Tulis alamat lengkap sesuai domisili]

Dengan ini mengajukan permohonan/perpanjangan*) Surat Tanda Registrasi Auditor Aplikasi SPBE.
Bersama ini kami sampaikan pula kelengkapan dokumen dalam bentuk *hardcopy* dan/atau *softcopy*.
Kami bertanggung-jawab atas kebenaran dari dokumen dan/atau data-data yang dipersyaratkan.

[Nama Kota, Tanggal Bulan Tahun]
Pemohon
[Nama]

BUPATI KOTAWARINGIN TIMUR,

HALIKINNOR

LAMPIRAN III : PERATURAN BUPATI KOTAWARINGIN TIMUR
NOMOR 58 TAHUN 2024
TENTANG PEDOMAN AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I
AUDIT INTERNAL KEAMANAN SPBE

1.1. Pendahuluan

Audit internal Keamanan SPBE adalah proses penilaian secara sistematis melalui verifikasi dan klarifikasi informasi yang dapat dilanjutkan dengan validasi informasi terhadap hasil Penilaian Mandiri untuk mengukur tingkat kematangan penerapan Keamanan SPBE.

1.2. Tujuan

Peraturan tentang Audit Internal Keamanan SPBE di lingkungan Pemerintah Daerah bertujuan untuk:

a. mewujudkan Audit Internal Keamanan SPBE yang sesuai standar; dan
b. mewujudkan keseragaman tata cara pelaksanaan Audit Keamanan SPBE.

1.3. Ruang lingkup

Peraturan Audit Internal Keamanan SPBE di lingkungan Pemerintah Daerah meliputi:

a. pelaksana;
b. domain;
c. standar Audit Keamanan SPBE; dan
d. tata cara Audit Keamanan SPBE; dan
e. sumber daya Audit Keamanan SPBE.

BAB II
PELAKSANA

Audit Internal Keamanan SPBE di lingkungan Pemerintah Daerah oleh Tim Auditor Internal Keamanan SPBE Daerah, sedangkan Audit Keamanan Eksternal SPBE di Lingkungan Pemerintah Daerah dilaksanakan oleh LAKI bidang SPBE yang terdiri atas:

a. BSSN; dan
b. LAKI bidang SPBE yang terakreditasi.

BSSN dan LAKI SPBE melaksanakan Audit Keamanan SPBE untuk cakupan Aplikasi Umum dan Aplikasi Khusus serta Infrastruktur SPBE di lingkungan Pemerintah Daerah sesuai dengan cakupan masing-masing.

BAB III
DOMAIN

3.1. Domain Audit Internal Keamanan SPBE terdiri atas:
   a. audit atas keamanan Aplikasi SPBE; dan/atau
   b. audit atas keamanan Infrastruktur SPBE.

   Kedua domain tersebut dapat disertai dengan pelaksanaan audit internal atas manajemen keamanan SPBE.
3.2. Pelaksanaan audit internal atas manajemen keamanan SPBE ditentukan oleh Pemerintah Daerah dengan mempertimbangkan kebutuhan akan pelaksanaan evaluasi atas manajemen keamanan SPBE di Pemerintah Daerah.
3.3. Audit internal atas Keamanan Aplikasi SPBE harus mencakup kepada pengujian atas kontrol keamanan dalam:
   a. perencanaan Aplikasi SPBE;
   b. pengembangan Aplikasi SPBE;
   c. operasional Aplikasi SPBE; dan
   d. pemantauan Aplikasi SPBE.
3.4. Audit internal atas Keamanan Infrastruktur SPBE terdiri atas:
   a. audit atas Pusat Data Nasional yang dimanfaatkan oleh Pemerintah Daerah;
   b. audit atas Sistem Penghubung Layanan; dan
   c. audit atas Jaringan Intra Pemerintah Daerah.
3.5. Audit atas Keamanan Pusat Data Nasional yang dimanfaatkan oleh Pemerintah Daerah harus mencakup kepada pengujian atas kontrol keamanan dalam:
   a. perencanaan Pemanfaatan Pusat Data Nasional oleh Pemerintah Daerah;
   b. pengembangan Pemanfaatan Pusat Data Nasional oleh Pemerintah Daerah;
   c. operasional Pemanfaatan Pusat Data Nasional oleh Pemerintah Daerah; dan
   d. pemantauan Pemanfaatan Pusat Data Nasional oleh Pemerintah Daerah.
3.6. Audit atas Keamanan Sistem Penghubung Layanan harus mencakup kepada pengujian atas kontrol keamanan dalam:
   a. perencanaan Sistem Penghubung Layanan;
   b. pengembangan Sistem Penghubung Layanan;
   c. operasional Sistem Penghubung Layanan; dan
   d. pemantauan Sistem Penghubung Layanan.
3.7. Audit atas Keamanan Jaringan Intra harus mencakup kepada pengujian atas kontrol keamanan dalam:
   a. perencanaan Jaringan Intra;
   b. pengembangan Jaringan Intra;
   c. operasional Jaringan Intra; dan
   d. pemantauan Jaringan Intra.
3.8. Audit atas manajemen keamanan SPBE terdiri atas:
   a. audit atas tata kelola keamanan SPBE;
   b. audit atas sistem manajemen keamanan SPBE; dan

c. audit atas kontrol keamanan SPBE.

Kontrol keamanan SPBE dipilih berdasarkan analisis risiko keamanan.

3.9. Audit atas Tata Kelola Keamanan SPBE harus mencakup kepada pengujian atas kontrol terhadap:
   a. pengevaluasian tata kelola keamanan SPBE;
   b. pengarahan tata kelola keamanan SPBE;
   c. pemantauan tata kelola keamanan SPBE;
   d. komunikasi tata kelola keamanan SPBE; dan
   e. asuransi/jaminan tata kelola Keamanan SPBE.

3.10. Audit atas sistem manajemen keamanan SPBE harus mencakup kepada pengujian atas kontrol terhadap:
   a. perencanaan sistem manajemen Keamanan SPBE;
   b. pengembangan sistem manajemen Keamanan SPBE;
   c. pelaksanaan sistem manajemen Keamanan SPBE;
   d. evaluasi sistem manajemen Keamanan SPBE; dan
   e. peningkatan sistem manajemen Keamanan SPBE.

3.11. Audit atas Pengendalian Keamanan SPBE dapat mencakup pengujian atas kontrol terhadap:
   a. kebijakan keamanan;
   b. organisasi keamanan;
   c. keamanan personil;
   d. keamanan aset;
   e. keamanan akses;
   f. keamanan kriptografi;
   g. keamanan fisik dan lingkungan;
   h. keamanan operasional;
   i. keamanan komunikasi;
   j. keamanan pengembangan dan pemeliharaan;
   k. keamanan rekanan;
   l. insiden keamanan;
   m. keamanan kontinuitas; atau
   n. kepatuhan kemanan.

BAB IV
STANDAR AUDIT INTERNAL KEAMANAN SPBE

Standar yang digunakan sebagai kriteria dalam Audit Internal Keamanan SPBE mencakup :

a. Pedoman Audit Keamanan SPBE yang dikeluarkan oleh Badan Riset dan Inovasi Nasional (BRIN);
b. Standar Nasional Indonesia; dan
c. Peraturan Bupati.

4.1. Audit Internal Keamanan SPBE menghasilkan kesimpulan:
   a. memadai;
   b. perlu peningkatan; atau
   c. tidak memadai.

4.2. kesimpulan Audit Internal Keamanan SPBE didapatkan dengan memperhatikan:

a. hasil evaluasi desain kontrol Keamanan SPBE dibandingkan dengan standar yang digunakan sebagai kriteria audit;
b. hasil evaluasi implementasi kontrol Keamanan SPBE dibandingkan dengan desain kontrol keamanan SPBE; dan
c. hasil evaluasi efektivitas kontrol Keamanan SPBE dibandingkan dengan tujuan kontrol keamanan SPBE.

Penarikan kesimpulan Audit Internal Keamanan SPBE mengacu pada Matriks Kesimpulan Audit Internal Keamanan SPBE berikut ini:

Hasil Evaluasi Desain Kontrol	Hasil Evaluasi Implementasi Kontrol	Hasil Pengujian Terinci Efektivitas Kontrol	Kesimpulan Audit Keamanan SPBE
Memadai	Sesuai dengan desain kontrol	Efektif	Memadai
		Perlu peningkatan	Memadai
		Belum efektif	Perlu peningkatan
	Tidak sesuai dengan desain kontrol	Efektif	Perlu peningkatan
		Perlu peningkatan	Tidak memadai
		Belum efektif	Tidak memadai
Perlu peningkatan	Sesuai dengan desain kontrol	Efektif	Memadai
		Perlu peningkatan	Perlu peningkatan
		Belum efektif	Tidak memadai
	Tidak sesuai dengan desain kontrol	Efektif	Tidak memadai
		Perlu peningkatan	Tidak memadai
		Belum efektif	Tidak memadai
Tidak memadai		Efektif	Tidak memadai
		Perlu peningkatan	Tidak memadai
		Belum efektif	Tidak memadai

BAB V
TATA CARA AUDIT KEAMANAN SPBE

5.1. Tata cara Audit Internal Keamanan SPBE terdiri atas:
a. penugasan;
b. perencanaan;
c. pelaksanaan;
d. supervisi;
e. pelaporan; dan
f. tindak lanjut.

5.2. Penugasan Audit Internal Keamanan SPBE dilakukan oleh Bupati atau Koordinator SPBE dengan menerbitkan surat tugas Audit Keamanan SPBE. Surat tugas Audit Keamanan SPBE mencakup informasi tentang:

a. Nama Auditor;
b. Jabatan dalam tim Audit Keamanan SPBE;
c. *Auditee*;
d. Domain Audit Keamanan SPBE;
e. Lokasi Audit Keamanan SPBE; dan
f. Waktu Audit Keamanan SPBE.

5.3. Perencanaan Audit Internal Keamanan SPBE dilakukan oleh tim Audit Internal Keamanan SPBE dengan menyusun Perencanaan Audit Keamanan SPBE. Perencanaan Audit Keamanan SPBE mencakup:
a. analisis risiko keamanan SPBE;
b. penentuan kriteria Audit Keamanan SPBE; dan
c. rencana pengujian Audit Keamanan SPBE.

Analisis risiko keamanan SPBE merupakan proses identifikasi dan evaluasi risiko keamanan SPBE yang relevan dengan domain Audit Keamanan SPBE.

Penentuan kriteria Audit Keamanan merupakan proses identifikasi dan pemetaan kriteria kontrol keamanan SPBE yang sesuai dengan domain Audit Keamanan SPBE.

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

5.4. Pelaksanaan Audit Internal Keamanan SPBE paling sedikit mencakup prosedur:
a. pemahaman kontrol keamanan SPBE:
b. evaluasi desain kontrol keamanan SPBE:
c. pengujian implementasi kontrol keamanan SPBE, dan/atau
d. pengujian terinci efektivitas kontrol keamanan SPBE.

Pemahaman kontrol keamanan SPBE merupakan prosedur yang dilakukan Auditor dalam mengidentifikasi informasi terdokumentasi untuk memperoleh pemahaman yang memadai tentang kontrol keamanan SPBE.

Evaluasi desain kontrol keamanan SPBE emrupakan prosedur yang dilakukan Auditor untuk memperoleh keyakinan yang memadai bahwa desain kontrol keamanan SPBE telah sesuai dengan kriteria kontrol keamanan SPBE yang digunakan.

Pengujian implementasi kontrol keamanan SPBE merupakan prosedur yang dilakukan Auditor untuk memperoleh keyakinan yang memadai bahwa implementasi kontrol telah sesuai dengan desain kontrol yang ada.

Pengujian terinci efektivitas pengendalian keamanan SPBE merupakan prosedur yang dilakukan Auditor untuk:
a. memperoleh keyakinan yang memadai bahwa kontrol keamanan SPBE telah dapat mencapai tujuannya dengan efektif, atau
b. mengidentifikasi risiko yang terjadi karena adanya kelemahan desain dan/atau implementasi kontrol keamanan SPBE.

5.5. Tim Audit Internal Keamanan SPBE menggunakan Pertimbangan Profesional untuk menentukan simpulan dari hasil prosedur:
a. evaluasi desain kontrol keamanan SPBE;

b. pengujian implementasi kontrol keamanan SPBE; dan
c. pengujian terinci efektivitas kontrol keamanan SPBE.

5.6. Simpulan dari hasil prosedur evaluasi desain kontrol keamanan SPBE terdiri atas:
a. memadai;
b. perlu peningkatan; atau
c. tidak memadai.

Simpulan menentukan prosedur Audit Keamanan SPBE setelah evaluasi desain kontrol keamanan SPBE, yaitu:
a. jika memadai, maka tim Audit Internal Keamanan SPBE melakukan prosedur pengujian implementasi kontrol keamanan SPBE dengan cakupan uji petik yang cukup;
b. jika perlu peningkatan, maka tim Audit Internal Keamanan SPBE melakukan prosedur pengujian implementasi kontrol keamanan SPBE dengan cakupan uji petik yang ekstensif; atau
c. jika tidak memadai, maka tim Audit Internal Keamanan SPBE tidak perlu melakukan prosedur pengujian implementasi kontrol keamanan SPBE dan langsung melakukan prosedur pengujian terinci efektivitas kontrol keamanan SPBE.

5.7. Simpulan dari hasil prosedur evaluasi desain kontrol keamanan SPBE terdiri atas:
a. sesuai dengan desain kontrol; atau
b. tidak sesuai dengan desain kontrol.

Simpulan sebagaimana dimaksud menentukan prosedur Audit Keamanan SPBE setelah pengujian implementasi kontrol keamanan SPBE, yaitu:
a. jika sesuai dengan desain kontrol, maka tim Audit Intrernal Keamanan SPBE melakukan prosedur pengujian terinci efektivitas kontrol keamanan SPBE dengan cakupan uji petik yang cukup; atau
b. jika tidak sesuai dengan desain kontrol, maka tim Audit Internal 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.

5.8. Simpulan dari hasil prosedur pengujian terinci efektivitas kontrol keamanan SPBE terdiri atas:
a. efektif;
b. perlu peningkaan; atau
c. belum efektif.

5.9. Supervisi Audit Keamanan SPBE mencakup:
a. supervisi aspek mutu Audit Keamanan SPBE; dan
b. supervisi aspek teknis Audit Keamanan SPBE.

Supervisi aspek mutu Audit Keamanan SPBE merupakan prosedur yang dilakukan oleh LATIK Keamanan SPBE untuk memastikan bahwa pelaksanaan setiap Audit Keamanan SPBE telah sesuai dengan pedoman kendali mutu Audit Keamanan SPBE yang dimiliki LATIK cakupan Keamanan SPBE.

Supervisi aspek teknis Audit Keamanan SPBE merupakan prosedur yang dilakukan oleh LATIK cakupan Keamanan SPBE untuk

memastikan bahwa pelaksanaan setiap Audit Keamanan SPBE telah memadai secara teknis sesuai dengan domain Audit Keamanan SPBE.

Supervisi Audit Keamanan SPBE dilakukan sesuai dengan metodologi dan sumber daya yang dimiliki LATIK cakupan Keamanan SPBE.

5.10. Pelaporan Audit Internal Keamanan SPBE dilakukan oleh tim Audit Internal Keamanan SPBE dengan menyusun Laporan Hasil Audit Internal. Laporan Hasil Audit Internal mencakup:
a. kondisi yang memerlukan perhatian pimpinan Daerah;
b. risiko atau potensi risiko yang diidentifikasi;
c. kriteria kontrol keamanan SPBE yang digunakan sesuai dengan domain Audit Keamanan SPBE;
d. rekomendasi tindakan perbaikan yang dapat dilakukan oleh Daeah.

Kondisi yang memerlukan perhatian pimpinan Daerah mencakup:
a. kelemahan dalam desain kontrol keamanan SPBE dibandingkan dengan kriteria kontrol keamanan SPBE yang digunakan; dan
b. ketidaksesuaian antara implementasi kontrol keamanan SPBE dengan desain kontrol keamanan SPBE.

Risiko atau potensi risiko yang diidentifikasi terdiri atas:
a. kelemahan desain dan/atau implementasi kontrol keamanan SPBE; dan
b. hasil pelaksanaan pengujian terinci kontrol keamanan SPBE.

Rekomendasi tindakan perbaikan yang dapat dilakukan oleh Daerah dilakukan untuk meningkatkan:
a. kecukupan desain kontrol keamanan SPBE;
b. kesesuaian implementasi kontrol keamanan SPBE; dan
c. efektivitas kontrol keamanan SPBE.

Rencana tindak lanjut dari Daerah disusun untuk memastikan tindak lanjut:
a. dilakukan secara tepat waktu;
b. mempertimbangkan risiko, manfaat dan biaya; dan
c. sesuai dengan ketentuan peraturan perundang-undangan.

Daerah mengirimkan Laporan Hasil Audit pada BSSN paling lambat 15 (lima belas) hari kerja sejak Laporan Hasil Audit diterbitkan.

5.11. Tindak lanjut Audit Internal Keamanan SPBE dilakukan oleh Pemerintah Daerah/SKPD/*Auditee*. Auditor internal berikutnya mengevaluasi hasil tindak lanjut Audit Internal Keamanan SPBE yang dilakukan oleh Pemerintah Daerah/SKPD/*Auditee*. Pemerintah Daerah/SKPD/*Auditee* melakukan pemantauan atas pelaksanaan rencana tindak lanjut tersebut.

5.12. Auditor berhak:
a. memperoleh informasi, data, dan dokumen lain yang lengkap dan benar dari Daerah sesuai dengan keperluan dan ketentuan peraturan perundang-undangan;
b. menerima imbalan hasil kerja sesuai dengan perjanjian kerja dan/atau ketentuan peraturan perundang-undangan; dan
c. mendapatkan pembinaan dan kesempatan dalam meningkatkan kompetensi profesi Auditor.

5.13. Auditor berkewajiban:

a. melakukan Audit Keamanan SPBE sesuai dengan prinsip Audit Keamanan SPBE;
b. melaksanakan Audit Keamanan SPBE sesuai dengan standar kinerja Audit Keamanan SPBE;
c. melakukan Audit Keamanan SPBE sesuai kompetensi yang dimiliki;
d. menyelesaikan pekerjaan sesuai dengan perjanjian kerja dengan Daerah; dan
e. menaati ketentuan peraturan perundang-undangan.

5.14. Auditor dilarang melanggar prinsip perlindungan terhadap keamanan informasi dari kebocoran dan penyalahgunaan informasi untuk kepentingan tertentu.

BAB VI
SUMBER DAYA AUDIT KEAMANAN SPBE

6.1. LATIK cakupan Keamanan SPBE harus mengalokasikan sumber daya Audit Keamanan SPBE dengan memadai.

6.2. Dalam mengalokasi sumber daya Audit Keamanan SPBE sebagaimana dimaksud pada ayat (1) LATIK cakupan Keamanan SPBE menentukan:
a. jumlah Auditor;
b. jumlah hari pelaksanaan Auditor Keamanan SPBE; dan
c. alat bantu Audit Keamanan SPBE.

6.3. Jumlah Auditor paling sedikit berjumlah 2 (dua) orang dalam satu penugasan dan dapat ditambah sesuai kebutuhan. Kebutuhan dengan memperhatikan paling sedikit:
a. kompetensi yang dibutuhkan sesuai domain audit; dan
b. kompleksitas teknologi dalam domain audit.

6.4. Jumlah hari pelaksanaan Audit Keamanan SPBE ditentukan dengan memperhatikan paling sedikit:
a. kompleksitas domain audit;
b. kompleksitas teknologi domain audit; dan
c. sebaran lokasi domain audit.

Jumlah hari pelaksanaan Audit Keamanan SPBE dapat mengacu pada matriks jumlah hari pelaksanaan Audit Keamanan SPBE berikut ini:

MATRIKS JUMLAH HARI PELAKSANAAN AUDIT KEAMANAN SPBE

Kompleksitas Domain Audit	Kompleksitas Teknologi Domain Audit Keamanan SPBE	Sebaran Lokasi Domain Audit Keamanan SPBE	Jumlah Hari*
Sederhana	Sederhana	Terpusat	1-2
		Tersebar	2-3
	Sedang	Terpusat	2-3
		Tersebat	3-4
	Kompleks	Terpusat	3-4
		Tersebar	4-5
Sedang	Sederhana	Terpusat	4-5
		Tersebar	5-6

	Sedang	Terpusat	5-6
		Tersebar	6-7
	Kompleks	Terpusat	6-7
		Tersebar	7-8
Kompleks	Sederhana	Terpusat	7-8
		Tersebar	8-9
	Sedang	Terpusat	8-9
		Tersebar	9-10
	Kompleks	Terpusat	9-10
		tersebar	>10

* Untuk satu tim paling sedikit terdiri atas dua orang Auditor.

6.5. Kompleksitas domain audit dapat mengacu pada Matriks Kompleksitas Domain Audit berikut:

MATRIKS KOMPLEKSITAS DOMAIN AUDIT KEAMANAN SPBE

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

6.6. Kompleksitas teknologi domain audit dapat mengacu pada Matriks Kompleksitas Teknologi Domain Audit berikut ini:

MATRIKS KOMPLEKSITAS TEKNOLOGI
DOMAIN AUDIT KEAMANAN SPBE

Indikator	Tingkat Kompleksitas Teknologi		
	Sederhana	Sedang	Kompleks
UMUM			
Jumlah Personil TI	< 5 orang	6-10 orang	> 10 orang
Jumlah Pengguna	< 100 pengguna	100-1000 pengguna	> 1000 pengguna
Jenis Dampak Kegagalan	Operasional saja	Operasional dan Finansial	Operasional, Finansial dan Legal
APLIKASI			
Sebaran peladen	Terpusat	Terdistribusi Dalam Negeri	Terdistribusi Dalam & Luar Negeri

Platform Teknologi	1 jenis	2-3 jenis	> 3 jenis
Waktu pengembangan	< 3 bulan	3-12 bulan	> 12 bulan
Indikator	Tingkat Kompleksitas Teknologi		
	Sederhana	Sedang	Kompleks
Usia Sistem	< 1 tahun	1-3 tahun	> 3 tahun
Transaksi per hari	< 5000	5000 s.d 50.000	> 50.000
Pola Pemrosesan	*Batch*	*Realtime*	*Hybrid*
Cakupan Proses Bisnis	< 30 %	30-60%	> 60 %
INFRASTRUKTUR – PUSAT DATA NASIONAL			
Pengelolaan	Alih Daya, Sewa	Mandiri	Campuran
Strata SNI	Strata 1-2	Strata 3	Strata 4
Sertifikasi	Belum ada	SNI 270001	SNI 270001 dan Standar Lain
INFRASTRUKTUR – JARINGAN INTRA			
Pengelolaan	Alih Daya, Sewa	Mandiri	Campuran
Cakupan Jaringan	*Local Area Network, Cluster Area Network*	*Metropolitian Area Network, Virtual Private Network*	*wide Area Network, Nasional*
Media Jaringan	Kabel	Nirkabel	Kabel & Nirkabel
INFRASTRUKTUR – SISTEM PENGHUBUNG LAYANAN			
Cakupan Sistem	Intra Instansi Pusat atau Intra Pemerintah Daerah	Antar Instansi Pusat atau Antar Pemerintah Daerah	Nasional
Sifat Sistem	Tertutup	Semi Terbuka	Terbuka
Konten Sistem	Data	Aplikasi	Layanan
Sifat Informasi	Terbuka	Terbatas	Tertutup

6.7. Sebagai lokasi domain audit dibedakan berdasarkan lokasi fisik yaitu:
   a. Terpusat; dan
   b. Tersebar.

6.8. Alat bantu Audit Keamanan SPBE merupakan perangkat teknologi yang digunakan Auditor dalam pelaksanaan pengujian kontrol keamanan.

6.9. Dalam menentukan penggunaan alat bantu Audit, LATIK Keamanan SPBE harus memperhatikan:
   a. Kompleksitas teknologi dalam domain audit; dan
   b. Keamanan alat bantu audit yang digunakan.

6.10. Format Laporan Pelaksanaan Latik Cakupan Keamanan SPBE terakreditasi adalah sebagai berikut:

KOP SURAT LATIK cakupan Keamanan SPBE Terakreditasi

LAPORAN LATIK CAKUPAN KEAMANAN SPBE TERAKREDITASI
TENTANG HASIL AUDIT KEAMANAN SPBE

BAB I PENDAHULUAN

A. Latar Belakang
B. Tujuan
C. Ruang Lingkup
D. Sasaran
E. Keluaran
(*output*)
F. Hasil yang diharapkan (*outcome*)

BAB II LAPORAN KEGIATAN

A. Identitas LATIK		
Nama LATIK	(isi nama Lembaga Pelaksana Audit)	
Periode Pelaporan	(isi periode pelaporan)	
Perubahan Keanggotaan Auditor	(isi jika ada perubahan dalam keanggotaan Auditor)	
B. Penanggungjawab Penyelenggaraan Audit		
Nama	(isi nama lengkap)	
Jabatan	(isi jabatan resmi)	
NIP/NIK	(isi Nomor Induk Pegawai/Nomor Induk Kependudukan)	
Kontak	(isi nomor telepon dan surel penanggungjawab)	
C. Penyelenggara Audit		
1. Umum		
Judul Audit TIK	(isi judul)	
Tanggal Laporan Audit	(isi tanggal)	
Jenis Audit	(isi jenis audit)	
2. Ringkasan Hasil Audit		
Ringkasan Temuan (parameter)	Ringkasan Rekomendasi (parameter)	
(temuan 1) jenis dan narasi	(rekomendasi 1) narasi singkat dan tenggat waktu	
(temuan 2)	(rekomendasi 2)	
D. Informasi Tindak Lanjut Audit		
Rekomendasi #1	Tenggat waktu	Tindak Lanjut #1
Rekomendasi #2	Tenggat waktu	Tindak Lanjut #2

Rekomendasi #3	Tenggat waktu	Tindak Lanjut #3

BAB III PENUTUP

[Pimpinan LATIK Cakupan Keamanan SPBE Terakreditasi],

[Nama]

BUPATI KOTAWARINGIN TIMUR,

HALIKINNOR

LAMPIRAN IV : PERATURAN BUPATI KOTAWARINGIN TIMUR
NOMOR 58 TAHUN 2024
TENTANG PEDOMAN AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

KRITERIA PENILAIAN
AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

I. Audit Internal TIK Infrastruktur SPBE

1. Pusat Data

Tahapan 1	**Perencanaan**
Aktivitas 1	Analisis Kebutuhan
1	Apakah sudah menyusun dokumen rencana pertumbuhan (*growth plan*) Pusat Data, seperti beban daya, pendingin, ruangan, dan lain-lain?
2	Apakah sudah ada kebijakan untuk melakukan analisis kebutuhan layanan Pusat Data?
3	Apakah sudah memiliki ruang lingkup layanan Pusat Data dari sisi cakupan geografis jenis industri yang dilayani?
4	Apakah sudah memiliki dokumen tentang jenis layanan yang dibutuhkan di Pusat Data/
5	Apakah memiliki prosedur pelaporan masalah yang terjadi di Pusat Data?
Aktivitas 2	Pengelolaan Lokasi
1	Apakah bangunan Pusat Data berada pada lokasi yang aman dari bahaya seperti bencana alam, polusi, interferensi elektromagnetik, getaran, dan lain-lain?
2	Apakah bangunan Pusat Data mempunyai akses jalan yang cukup dan fasilitas parkir?
3	Apakah lokasi Pusat Data memiliki temperatur sekitar yang rendah dan tidak berada di kawasan yang memiliki kelembaban yang tinggi?
4	Apakah Penyelenggara Pusat Data sudah memilih lokasi Pusat Data yang aman dari bencana, mudah diakses, dan mudah melakukan pengembangan/pembangunan Pusat Data?
Aktivitas 3	Pengelolaan Bangunan
1	Apakah ruang komputer tidak berada di bawah area perpipaan (*plumbing*) yang berbahaya?
2	Apakah jendela ruang komputer yang menghadap ke sinar matahari sudah ditutup untuk mencegah panas?
3	Apakah Pusat Data memiliki area bongkar muat yang memadai untuk menangani penghantaran barang/peralatan?

4	Apakah Pusat Data memiliki akses/jalur penyelamatan jika terjadi bahaya/ancaman?
Aktivitas 4	Pengelolaan Kebakaran
1	Apakah jumlah dan lokasi pintu darurat kebakaran sudah sesuai dengan ketentuan peraturan perundang-undangan?
2	Apakah pintu darurat kebakaran dapat dibuka ke arah luar?
3	Apakah semua tanda peringatan kebakaran sudah ditempatkan pada posisinya sesuai ketentuan peraturan perundang-undangan?
4	Apakah bangunan sudah dilengkapi dengan sistem proteksi petir?
Aktivitas 5	Pengelolaan Kelistrikan
1	Apakah Pusat Data menyediakan ruang panel kelistrikan?
2	Apakah sudah tersedia catu daya listrik alternatif (seperti generator) dengan kapasitas yang memadai untuk operasional Pusat Data paling sedikit 6 (enam) jam selama kejadian gangguan listrik utama?
3	Apakah perangkat Pusat Data sudah diproteksi dengan UPS atau catu daya cadangan lainnya?
4	Apakah Pusat Data memiliki perhitungan efisiensi pemakaian listrik pada pusat data (*Power Usage Effectiveness*) terhadap keseluruhan beban daya maksimum Pusat Data?
Aktivitas 6	Pengelolaan Suhu Ruangan
1	Apakah ruang komputer sudah dijaga dan dikendalikan temperatur dengan suhu antara 18-24°C?
2	Apakah ruang komputer sudah dijaga dan dikendalikan kelembaban ruangannya dengan kelembaban antara 50-55%?
3	Apakah peralatan pengkondisian udara sudah dihubungkan ke catu daya utama dan didukung oleh catu daya alternatif?
Aktivitas 7	Pengelolaan Pengkabelan
1	Apakah seluruh pengkabelan interior dengan tipe tidak mudah terbakar (*low flammability*)?
2	Apakah setiap rak memiliki akses ke sistem saluran kabel, di atas atau di bawahnya, yang memungkinkan kabel-kabel dapat ditata secara baik antar rak?
3	Apakah kabel yang melewati dinding sudah dilindungi terhadap bahaya api sesuai ketentuan peraturan perundang-undangan?
4	Apakah kabel sudah tidak diletakkan di pintu, lantai, atau digantung antar rak?
5	Apakah setiap kabel sudah memiliki identifikasi yang unik pada kedua ujung awal dan akhir?
6	Apakah setiap rak peralatan sudah memiliki label identifikasi?

Aktivitas 8	Pengelolaan Pembagian Ruangan
1	Apakah sudah memiliki area server yang merupakan ruang penempatan rak server, server, *storage*, dan berbagai perangkat penunjang keberlangsungan operasi server seperti sistem pendingin, UPS, sistem pemadam api dan sistem catu daya listrik?
Aktivitas 9	Pengelolaan Sistem Pendinginan
1	Apakah Pusat Data memiliki dokumen spesifikasi teknis sistem pendingin, skema diagram sistem pendinginan, jaminan layanan purna jual, nomor kontak layanan, dan kontrak penawaran?
2	Apakah Pusat Data memiliki temperatur ruangan 18°C - 27°C?
3	Apakah Pusat Data memiliki tingkat perubahan temperatur ruangan per jam maksimum 5°C?
4	Apakah Pusat Data memiliki kelembaban ruangan: RH (*Relative Humidity*) ≤ 60%, titik embun: 5,5°C - 15°C?
5	Apakah memiliki prosedur pelaporan masalah yang terjadi di Pusat Data?
Aktivitas 10	Pengelolaan Sistem Jaringan Data
1	Apakah Pusat Data memiliki label kabel yang terdiri dari nomor rak dan nomor baris pada rak?
2	Apakah Pusat Data sudah memiliki *bandwidth* untuk keperluan komunikasi yang diperlukan dan memiliki jalur komunikasi data alternatif guna menghindari kepadatan lintas data serta mencegah kegagalan satu jalur (*single point of failure*)?
3	Apakah Pusat Data sudah menggunakan teknologi komputasi awan sehingga bagi pakai data, aplikasi, dan infrastruktur dapat dilakukan?
Tahapan 2	**Pengembangan**
Aktivitas 1	Implementasi
1	Apakah dalam mengembangkan Pusat Data sudah memiliki metode/standar tertentu sebagai acuan?
2	Apakah sudah ada dokumentasi selama pengembangan Pusat Data?
3	Apakah terdapat perubahan realisasi pengembangan Pusat Data dan sudah didokumentasikan?
4	Apakah pengembangan Pusat Data sudah memiliki rencana penerapan?
Aktivitas 2	Instalasi
1	Apakah sudah memiliki prosedur instalasi Pusat Data?
2	Apakah sudah memiliki daftar personil yang bertugas melakukan instalasi Pusat Data?
3	Apakah sudah memiliki rencana pelatihan terhadap personil yang melakukan instalasi Pusat Data?
4	Apakah sudah memiliki daftar fasilitas yang dibutuhkan

	selama instalasi Pusat Data?
Aktivitas 3	Pengujian
1	Apakah sudah memiliki rencana pengujian (*Test Plan*) terhadap Pusat Data?
2	Apakah sudah memiliki rancangan pengujian (*Test Design*) terhadap Pusat Data?
3	Apakah sudah memiliki prosedur pengujian (*Test Procedures*) terhadap Pusat Data?
4	Apakah sudah memiliki laporan pengujian (*Test Report*) terhadap Pusat Data?
Tahapan 3	**Pengoperasian**
Aktivitas 1	Organisasi
1	Apakah sudah memiliki struktur organisasi Pusat Data yang efektif dan efisien dengan klasifikasi tugas, distribusi dan hierarki kewenangan sesuai standar?
2	Apakah sudah mendefinisikan tugas, tanggung jawab dan ukuran kompetensi SDM Pusat Data?
3	Apakah disediakan ruang kendali untuk melakukan fungsi pemantauan dan pengendalian?
Aktivitas 3	Manajemen Operasi
1	Apakah sudah disediakan manual operasi umum yang mencakup seluruh persyaratan operasi Pusat Data?
2	Apakah seluruh perangkat utama seperti pengkondisi udara, UPS, generator, dan lain sebagainya sudah terdapat dalam pencatatan aset?
3	Apakah seluruh konfigurasi dan prosedur operasi termasuk di dalamnya: Perubahan Konfigurasi dan *Set-point Default* sudah didokumentasikan?
4	Apakah sudah memiliki informasi dokumentasi lokasi yang meliputi bangunan/lantai, lokasi rak, denah rak, dan interkonektivitas dan logik dari peralatan?
5	Apakah sudah tersedia daftar kontar tersedia yang mencatat seluruh staf Pusat Data, fungsi dan kontak rinci, pemasok, perusahaan pemeliharaan, dan layanan darurat?
6	Apakah sudah tersedia perencanaan tertulis yang mudah diakses untuk menjelaskan secara rinci status alarm dan bagaimana gangguan sistem ditangani oleh staf Pusat Data?
Aktivitas 4	Pusat Pemulihan Bencana
1	Apakah penyelenggara Pusat Data sudah memiliki Pusat Pemulihan Bencana?
2	Apakah penempatan fasilitas Pusat Pemulihan Bencana sudah mempertimbangkah hal-hal seperti: jarak terhadap lokasi Pusat Data yang meminimalkan risiko, biaya yang layak dan memenuhi *Service Level Agreement* (SLA) yang disyaratkan?
3	Apakah Penyelenggara Pusat Data sudah memiliki Rencana Kelangsungan Bisnis (*Business Continuity Plan*/BCP) untuk

	mempertahankan kelangsungan fungsi bisnis saat gangguan terjadi dan sesudahnya?
4	Apakah Penyelenggara Pusat Data sudah memiliki rencana (*Recovery Planning*/DRP) untuk memperbaiki operabilitas sistem target, aplikasi, dan fasilitas komputer di lokasi alternatif dalam kondisi darurat?
Aktivitas 5	Infrastruktur
1	Apakah Penuelenggara Pusat Data sudah menerapkan manajemen fasilitas Pusat Data seperti menyusun daftar perangkat/fasilitas, manajemen perawatan fasilitas, menyusun kontrak perawatan, memastikan ketersediaan dokumen manajemen dan pelaporan perawatan?
2	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen konfigurasi Pusat Data?
Aktivitas 6	Manajemen SDM Pusat Data
1	Apakah Penyelenggara Pusat Data sudah memiliki sistem manajemen untuk mengelola kompetensi sumber daya manusia dan tenaga ahli dalam rangka memastikan tersedianya layanan Pusat Data yang berkualitas?
2	Apakah Penyelenggara Pusat Data sudah memiliki program pelatihan karyawan sesuai dengan rencana peningkatan karir dan kompetensinya meliputi peraturan dan regulasi, keselamatan kerja, pengetahuan dan keterampilan dalam bidang tertentu, etika kerja, penanggulangan kondisi darurat, dan Standar Operasional Prosedur (SOP)?
3	Apakah Penyelenggara Pusat Data sudah menetapkan kebijakan dan mekanisme kerja untuk mengukur kinerja sumber daya manusia yang meliputi kompetensi yang diperlukan, rencana peningkatan, dan sasaran yang terukur?
Aktivitas 7	Monitoring, Pelaporan, dan Pengendalian
1	Apakah Penyelenggara Pusat Data sudah menerapkan monitoring, Pelaporan, dan Pengendalian?
Aktivitas 8	Manajemen Layanan Pusat Data
1	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen dokumen kelayanan?
2	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen keselamatan kerja untuk karyawan, tamu pengguna layanan pusat data, dan pengguna layanan pusat data yang menetap dan berada di lingkungan gedung pusat data pada saat kejadian insiden?
3	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen proyek?
Tahapan 4	**Pemeliharaan**
Aktivitas 1	Pemeliharaan
1	Apakah setiap staf Pusat Data dan/atau kontraktor yang bertugas dalam pemeliharaan memiliki kompetensi yang sesuai?

2	Apakah setiap peralatan yang membutuhkan pemeliharaan sudah memiliki daftar dan catatan pemeliharaan yang merinci peralatan, tanggal pemeliharaan, hasil dan kontak rinci?
3	Apakah sudah mendeskripsikan siklus hidup peralatan dan perangkat (identifikasi garansi/*lifetime*, perjanjian pemeliharaan, dan laporan kinerja peralatan)?
4	Apakah sudah memiliki SOP pemeliharaan komponen dan penggantian suku cadang sesuai standar?
5	Apakah sudah menyusun laporan perencanaan dan penjadwalan pemeliharaan komponen Pusat Data?
Aktivitas 2	Manajemen Konfigurasi Perangkat Keras/MKP (*Hardware Configuration Management*)
1	Apakah sudah ditentukan apa saja yang menjadi lingkup manajemen konfigurasi perangkat keras?
2	Bagaimana cara mengelola konfigurasi perangkat keras?
3	Apa saja aktivitas yang dilakukan pada proses manajemen konfigurasi perangkat keras?
4	Apakah sudah memiliki jadwal untuk melakukan proses manajemen konfigurasi perangkat keras?
5	Apakah sudah memiliki sumber daya untuk melakukan proses manajemen konfigurasi perangkat keras?
Aktivitas 3	Pemantauan
1	Apakah Pusat Data sudah memiliki analisis risiko yang meliputi risiko yang mungkin terjadi, dampak, dan strategi mengurangi risiko yang dipantau terus menerus?
2	Apakah seluruh perangkat kritis seperti status UPS, kondisi gangguan, dan lain-lain sudah dipantau secara kontinyu?
3	Apakah Pusat Data memiliki sistem monitoring lingkungan Pusat Data (*environtment monitoring system*) yang meliputi antara lain monitoring temperatur, kelembapan, asap, kebakaran, kebocoran air, dan tegangan listrik?
4	Apakah Penyelenggara Pusat Data sudah membuat laporan pemantauan yang meliputi tren laju pemanfaatan sumber daya listrik, pendingin, rak server, rekaman alarm, dan kejadian per periode?
5	Apakah efisiensi energi sudah dimonitor secara berkala sekurang-kurangnya 2 (dua) kali dalam 1 (satu) tahun dengan menggunakan acuan pengukuran *power usage effectiveness* (PUE)?

2. Jaringan Intra Pemerintah Daerah

Tahapan 1	**Perencanaan**
Aktivitas 1	Kebutuhan Bisnis (*Business Requirement*)
1	Apakah jaringan dapat menyampaikan solusi yang diperlukan untuk kebutuhan layanan SPBE?
2	Apakah sudah dijelaskan secara rinci apa yang dibutuhkan

	pengguna dan perannya dalam proses perencanaan jaringan?
3	Apakah sudah dijelaskan ruang lingkup jaringan yang direncanakan yang mencakup kebutuhan fungsional dan non-fungsional?
Aktivitas 2	Kebutuhan Jaringan (*Network Requirement*)
1	Apa saja proses-proses/fungsi/layanan yang dapat dilakukan oleh jaringan?
2	Apa sajakah kemampuan kerja yang dapat dicapai dan dilakukan oleh jaringan?
3	Apakah terdapat batasan khusus yang harus ada dalam rancangan jaringan?
Aktivitas 3	Rancangan Jaringan (*Network Design*)
1	Apa saja persiapan yang dilakukan dalam melakukan perancangan jaringan?
2	Apakah sudah dilakukan analisis lingkungan dalam melakukan perancangan jaringan?
3	Bagaimana dan seberapa besar cakupan dari jaringan yang akan dirancang?
Tahapan 2	**Pengembangan**
Aktivitas 1	Implementasi Jaringan (*Network Implementation*)
1	Apa sajakah metode-metode pengembangan yang digunakan dalam pengembangan jaringan?
2	Apakah sudah menyusun konfigurasi jaringan?
3	Apakah sudah menyusun Diagram LAN/Pengkabelan terkait pengembangan jaringan?
Aktivitas 2	Instalasi (*Installation*)
1	Apakah telah menyusun prosedur untuk instalasi jaringan?
2	Apakah telah menyusun dan menetapkan personil untuk instalasi jaringan?
3	Apakah telah menyusun rencana pelatihan personil untuk instalasi jaringan?
4	Apakah telah menyusun jadwal untuk instalasi jaringan?
5	Apakah telah menyiapkan fasiliats yang dibutuhkan untuk instalasi jaringan?
Aktivitas 3	Pengujian (*Testing*)
1	Apakah telah menyusun dokumen Rencana Pengujian dalam rangka pengembangan dan pengujian jaringan?
2	Apakah telah menyusun dokumen Rancangan Pengujian dalam rangka pengembangan dan pengujian jaringan?
3	Apakah telah menyusun dokumen Prosedur Pengujian dalam rangka pengembangan dan pengujian jaringan?
4	Apakah telah menyusun dokumen Laporan Pengujian dalam rangka pengembangan dan pengujian jaringan?
Tahapan 3	**Pengoperasian**
Aktivitas 1	Utilisasi/Kinerja Jaringan (*Network Utilization/Performance*)
1	Apakah telah menyusun dan menyediakan pedoman

	penggunaan Jaringan dan Perangkat Keras (instalasi, akses, navigasi, utilisasi, dan *report*) dalam rangka pengoperasian jaringan?
2	Apakah telah menyusun dan menyediakan Fasilitas Bantuan yang membantu petugas dalam mengoperasikan jaringan?
Tahapan 4	**Pemeliharaan**
Aktivitas 1	Pemeliharaan Jaringan (*Network Maintenance*)
1	Apakah telah menentukan ruang lingkup tanggung jawab pemeliharaan jaringan?
2	Apakah telah menentukan urutan proses pemeliharaan jaringan?
3	Apakah telah membentuk tim dan personil yang akan melakukan pemeliharaan jaringan?
Aktivitas 2	Manajemen Konfigurasi Jaringan/MKJ (*Network Configuration Management*)
1	Apakah sudah ditentukan apa saja yang menjadi lingkup manajemen konfigurasi jaringan?
2	Apa saja aktivitas yang dilakukan pada proses manajemen konfigurasi jaringan?
3	Apakah sudah memiliki sumber daya untuk melakukan proses manajemen konfigurasi jaringan?

3. Sistem Penghubung Layanan

Tahapan 1	**Perencanaan**
Aktivitas 1	Prinsip
1	Dapat digunakan kembali (*reusable*) agar dapat dimanfaatkan secara berulang tanpa perlu dikembangkan lagi oleh pihak yang membutuhkan?
2	Dapat dikembangkan lebih lanjut tanpa perlu melibatkan pengembang awal?
3	Dapat diperiksa (*auditable*) dan memiliki kemudahan bagi yang memiliki kewenangan untuk melakukan pengamanan, verifikasi, pengujian, dan pemeriksaan terhadapnya?
4	Dapat diawasi dan dinilai tingkat pemanfaatannya?
5	Dapat dibagikan antar Sistem Elektronik yang berbeda karakteristik?
Aktivitas 2	Kebijakan
1	Memiliki kajian kebutuhan penerapan Sistem Penghubung sekurang-kurangnya meliputi Dasar Hukum Pertimbangan, Pihak yang terkait, Manfaat, dan Ruang Lingkup?
Aktivitas 3	Kebijakan
1	Memiliki satuan kerja yang bertugas untuk memastikan penerapan Sistem Penghubung?
2	Memiliki sumber daya manusia yang kompeten di bidang Sistem Penghubung?
Aktivitas 4	Teknis
1	Dikembangkan dalam bentuk antarmuka pemrograman

	aplikasi?
2	Memiliki kemampuan untuk menjaga keberlangsungan dan ketersediaan interoperabilitas data?
3	Memiliki infrastruktur yang sesuai dengan kebutuhan kapasitas dan tingkat layanan?
4	Memiliki panduan teknis dan pendauan penggunaan Sistem Penghubung yang terpelihara dan terjaga keterkinian/keterbaruannya?
Tahapan 2	**Pengembangan**
Aktivitas 1	Implementasi
1	Apakah dalam mengembangkan Sistem Penghubung sudah memiliki metode/standar tertentu sebagai acuan?
2	Apakah sudah ada dokumentasi rancangan pengembangan Sistem Penghubung (*Development Design*)?
3	Apakah pengembangan Sistem Penghubung sudah memiliki rencana penerapan?
Aktivitas 2	Instalasi
1	Apakah sudah memiliki prosedur instalasi Sistem Penghubung?
2	Apakah sudah memiliki daftar personil yang bertugas melakukan instalasi Sistem Penghubung?
3	Apakah sudah memiliki rencana pelatihan terhadap personil yang melakukan instalasi Sistem Penghubung?
4	Apakah sudah memiliki jadwal instalasi Sistem Penghubung?
5	Apakah sudah memiliki fasilitas yang dibutuhkan selama instalasi Sistem Penghubung?
Aktivitas 3	Pengujian
1	Apakah sudah memiliki rencanan pengujian (*Test Plan*) terhadap Sistem Penghubung?
2	Apakah sudah memiliki rancangan pengujian (*Test Design*) terhadap Sistem Penghubung?
3	Apakah sudah memiliki prosedur pengujian (*Test Procedures*) terhadap Sistem Penghubung?
4	Apaah sudah memiliki laporan pengujian (*Test Report*) terhadap Sistem Penghubung?
Tahapan 3	**Pengoperasian**
Aktivitas 1	Penyelenggaraan
1	Sistem Penghubung dibangun dan dioperasikan oleh Penyelenggara Sistem Penghubung?
2	Sistem Penghubung dapat digunakan oleh Infrastruktur Instansi Daerah?
3	Sistem Penghubung yang digunakan oleh Infrastruktur Pemerintah Daerah sudah terhubung ke dalam Jaringan Intra Pemerintah?
4	Penyelenggaraan Sistem Penghubung oleh Infrastruktur Pemerintah Daerah dilaksanakan organisasi yang membidangi urusan komunikasi dan informatika?

Aktivitas 2	Dokumen Mekanisme Kerja
1	Memiliki Panduan Teknis (*Technical Guide*) yang berisi prosedur kerja?
2	Memiliki Panduan Pengguna (*User Guide*) yang berisi panduan penggunaan?
Tahapan 4	**Pemeliharaan**
Aktivitas 1	Pemeliharaan
1	Telah menentukan ruang lingkup tanggung jawab pemeliharaan Sistem Penghubung?
2	Telah menentukan urutan proses pemeliharaan Sistem Penghubung?
3	Telah membentuk tim dan personil yang akan melakukan pemeliharaan Sistem Penghubung?
4	Telah mengalokasikan sumber daya terkait dalam rangka mendukung proses pemeliharaan Sistem Penghubung?
5	Telah melakukan Pelacakan Kinerja pada Sistem Penghubung sebagai bagian dan proses pemeliharaan?

II. Audit Internal TIK Aplikasi SPBE

Tahapan 1	**Perencanaan**
Aktivitas 1	Persyaratan Layanan (*Business Requirement*)
1	Apakah aplikasi dapat menyampaikan solusi yang diperlukan untuk kebutuhan layanan?
2	Apakah aplikasi dapat menjelaskan secara rinci apa yang dibutuhkan pengguna dalam proses layanan?
Aktivitas 2	Kebutuhan Perangkat Lunak (*Software Requirement*)
3	Apa saja proses-proses/fungsi/layanan yang dapat dilakukan oleh aplikasi?
4	Bagaimana aplikasi menggambarkan antarmuka yang dapat berinteraksi/berhubungan dengan komponen aplikasi lainnya?
5	Apa sajakah kemampuan kerja yang dapat dicapai oleh aplikasi?
6	Apakah terdapat batasan khusus yang harus ada di dalam rancangan perangkat lunak?
Aktivitas 3	Rancangan Perangkat Lunak (*Software Design*)
7	Bagaimana bentuk deskripsi sistem dari aplikasi?
8	Bagaimana deskripsi rancangan basis data dari aplikasi?
9	Bagaimana bentuk arsitektur dari aplikasi sehingga dapat menggambarkan keseluruhan sistem, proses, dan layanan aplikasi?
10	Bagaimana gambaran dan karakteristik antarmuka dari aplikasi?
Tahapan 2	**Pengembangan**
Aktivitas 1	Implementasi Perangkat Lunak (*Software Implementation*)
11	Apa sajakah metode-metode pengembangan perangkat lunak yang digunakan dalam pengembangan aplikasi?
12	Apakah sudah memiliki dokumentasi dari kode-kode

	pengembangan perangkat lunak?
13	Apakah perangkat lunak dapat digunakan kembali secara berkesinambungan di masa yang akan datang?
14	Apakah kode sumber aplikasi dapat dimodifikasi/bersifat *open source*?
Aktivitas 2	Pengujian (*Testing*)
15	Apakah sudah memiliki rencana pengujian (*Test Plan*) terhadap aplikasi?
16	Apakah sudah memiliki rancangan pengujian (*Test Design*) terhadap aplikasi?
17	Apakah sudah memiliki rancangan atau rangkaian mengenai tindakan yang dilakukan oleh penguji/*tester*?
18	Apakah sudah memiliki prosedur-prosedur pengujian terhadap aplikasi?
19	Apakah sudah memiliki laporan pengujian terhadap aplikasi?
Aktivitas 3	Instalasi/Pemasangan (*Installation*)
20	Apakah sudah memiliki prosedur instalasi/pemasangan untuk aplikasi?
21	Apakah sudah memiliki daftar personil yang bertugas untuk melakukan instalasi/pemasangan aplikasi?
22	Apakah sudah memiliki rencana pelatihan terhadap personil yang melakukan instalasi/pemasangan aplikasi?
23	Apakah sudah memiliki jadwal instalasi/pemasangan aplikasi?
24	Apakah sudah memiliki daftar fasilitas yang dibutuhkan selama instalasi/pemasangan aplikasi?
Tahapan 3	**Pengoperasian**
Aktivitas 1	Penggunaan Perangkat Lunak (*Software Usage*)
25	Apakah aplikasi sudah bisa berkolaborasi dengan aplikasi lain?
26	Apakah aplikasi merupakan perangkat lunak yang dipersiapkan untuk dapat digunakan/diaplikasikan secara umum?
27	Apakah memiliki prosedur/petunjuk/manual penggunaan aplikasi?
28	Apakah penamaan perintah-perintah dalam perangkat lunak distandarkan/dibakukan?
29	Bagaimana respon aplikasi dalam menanggapi kesalahan dan apakah memiliki solusi terhadap permasalahan tersebut?
30	Apakah memiliki/menyediakan fasilitas bantuan dan dokumentasi mengenai pertanyaan yang sering diajukan (FAQ)
Tahapan 4	**Pemeliharaan**
Aktivitas 1	Pemeliharaan Perangkat Lunak (*Software Maintenance*)
31	Apakah sudah ditentukan lingkup apa saja yang akan dilakukan pada proses pemeliharaan aplikasi?

32	Apakah memiliki urutan/rangkaian proses pemeliharaan aplikasi?
33	Apakah sudah dibentuk tim/kelompok kerja untuk melaksanakan pemeliharaan aplikasi dengan klasifikasi tugas yang sudah ditentukan?
34	Apakah sudah ditentukan alokasi sumber daya untuk proses pemeliharaan aplikasi?
35	Apakah memiliki cara untuk dapat mengetahui, merekam, dan melacak kinerja dari aplikasi?
Aktivitas 2	Manajemen Konfigurasi Perangkat Lunak (*Software Configuration Management*)
36	Apakah sudah ditentukan apa saja yang menjadi ruang lingkup manajemen konfigurasi perangkat lunak?
37	Bagaimana cara mengelola konfigurasi perangkat lunak?
38	Apa saja aktivitas yang dilakukan pada proses manajemen konfigurasi perangkat lunak?
39	Apakah sudah memiliki jadwal untuk melakukan proses manajemen konfigurasi perangkat lunak?
40	Apakah sudah memiliki sumber daya untuk melakukan proses manajemen konfigurasi perangkat lunak?

III. Audit Internal TIK Keamanan SPBE

1. Audit Keamanan Pusat Data SPBE

PERENCANAAN	
1	Identifikasi keamanan lokasi dan lingkungan pusat data telah dilakukan?
2	Identifikasi keamanan jalur kabel jaringan data telah dilakukan?
3	Identifikasi keamanan jalur kabel listrik dan sistem kelistrikan pusat data telah dilakukan?
4	Identifikasi keamanan sistem pengendalian kebakaran telah dilakukan?
5	Identifikasi keamanan akses fisik gedung dan perimeter pusat data telah dilakukan?
PENGEMBANGAN	
1	Persyaratan untuk pengembangan pusat data dan berbagai fasilitas penunjangnya telah ditetapkan dan diterapkan?
2	Perubahan dan penyesuaian atas desain pusat data telah dikendalikan dengan menggunakan prosedur pengendalian perubahan yang formal?
3	Kegiatan pengembangan pusat data telah diawasi dan dipantau pihak organisasi?
4	Pengujian keamanan saat pengembangan pusat data telah dilakukan?
OPERASIONAL	
1	Pengunjung yang akan memasuki area pusat data telah dikendalikan dengan mendapatkan izin masuk dari penyelenggara pusat data?

2	Untuk memasuki area pusat data telah menggunakan sistem pengendali akses berupa kartu akses elektronik, biometrik atau pemindai jari?
3	Mobilisasi (keluar/masuk) perangkat pada pusat data telah dikendalikan dengan surat izin masuk/keluar barang, dilakukan melalui area bongkar muat dan melalui pemeriksaan fisik atas penerimaan dan pengiriman barang di pusat data?
PEMANTAUAN	
1	Pemantauan terhadap akses personil dan pengunjung pusat data telah dilakukan?
2	Pemantauan terhadap akses masuk dan keluar barang pada pusat data telah dilakukan?
3	Pemantauan terhadap kondisi lingkungan pusat data telah dilakukan mencakup suhu ruangan pusat data, kelembaban ruangan, kebocoran air, sistem pemantauan kebakaran, dan sensor panas dan sensor asap, ketersediaan pasokan listrik dan penggunaan daya listrik?

2. Audit Keamanan Jaringan Intra

PERENCANAAN	
1	Kebijakan tentang perencanaan, pengembangan, operasional, dan pemantauan keamanan Jaringan Intra?
2	Identifikasi penetapan peran, tanggung jawab, dan kewenangan dari pihak-pihak yang terkait dengan keamanan jaringan intra?
3	Pengendalian atas pembuatan, perubahan, dan penyimpanan dokumentasi kebijakan, standar, prosedur, desain arsitektur teknis, serta informasi lainnya terkait jaringan intra?
PENGEMBANGAN	
1	Pengendalian keamanan secara mendalam (*defense in depth*) terhadap ancaman keamanan dari internal maupun eksternal jaringan intra.
2	Standar spesifikasi dan konfigurasi teknis terkait desain perangkat jaringan dan perangkat keamanan jaringan terkait Jaringan Intra Pemerintah Daerah.
3	Pengendalian keamanan terhadap ancaman *malware* dan *intrusion* yang berasal dari internal maupun eksternal Jaringan Intra Pemerintah Daerah.
4	Pengendalian keamanan terkait Jaringan Intra terhadap berbagai kebutuhan bisnis, sekurang-kurangnya meliputi: a) Keamanan akses jarak jauh (*remote*/VPN); b) Keamanan akses jaringan ke instansi lain; c) Keamanan akses jaringan ke internet; d) Keamanan akses jaringan nirkabel.
OPERASIONAL	
1	Kebijakan terkait operasional keamanan Jaringan Intra

	bagi pengguna yang mencakup ketentuan pengguna Jaringan Intra yang aman, dan konsekuensi pelanggaran dan penyalahgunaan Jaringan Intra telah dilaksanakan.
2	Pengendalian integritas konfigurasi yang dapat mencegah adanya perubahan yang tidak sah terhadap konfigurasi perangkat terkait Jaringan Intra.
3	Pemeliharana perangkat terkait keamanan Jaringan Intra secara berkala untuk preventif maupun korektif.
4	Pengendalian keberlangsungan keamanan Jaringan Intra mencakup sekurang-kurangnya pencadangan konfigurasi dan perangkat terkait Jaringan Intra.
PEMANTAUAN	
1	Identifikasi perangkat jaringan dan keamanan jaringan terkait Jaringan Intra yang dilakukan pemantauan.
2	Identifikasi jenis informasi minimum yang harus terhadap dalam *audit log* pada perangkat jaringan dan keamanan jaringan terkait Jaringan Intra.
3	Penerapan *audit log* yang mencatat informasi dan kejadian yang terkait dengan keamanan Jaringan Intra yang sekurang-kurangnya meliputi: a) Waktu, sumber, dan tujuan; b) Ancaman dan/atau kejadian keamanan yang berasal dari internal maupun eksternal; c) Aktivitas-aktivitas anomali di luar kondisi normal operasional.
4	Pelaporan hasil pemantauan keamanan Jaringan Intra secara berkala dan terdokumentasi.

3. Audit Keamanan Sistem Penghubung Layanan

PERENCANAAN	
1	Kebijakan tentang keamanan dalam perencanaan, pengembangan, implementasi, dan operasional, serta pemantauan dan pemeliharaan aplikasi yang terdokumentasi.
2	Identifikasi, penetapan peran, tanggung jawab, dan kewenangan dari pihak-pihak yang terkait dengan keamanan aplikasi
3	Identifikasi standar kebutuhan dan persyaratan minimum keamanan aplikasi yang sekurang-kurangnya meliputi: a) Kebutuhan kerahasiaan dan privasi; b) Kebutuhan integritas; c) Kebutuhan ketersediaan dan kontinuitas; d) Kebutuhan otentifikasi; e) Kebutuhan otorisasi; f) Kebutuhan akuntabilitas dan *non-repudiation*; g) Kebutuhan peraturan, regulasi hukum, dan perundang-undangan yang berlaku.
4	Identifikasi kendali keamanan tambahan, jika aplikasi

	dikembangkan oleh pihak ketiga, meliputi: a) Hak kekayaan intelektual, kepemilikan aplikasi, dan kode sumber asli; b) Penyimpanan kode sumber asli berdasarkan hak kepemilikan; c) Kebijakan, prosedur, dan standar terkait keamanan aplikasi pada pihak ketiga; d) Hak untuk melakukan verifikasi dan validasi kendali keamanan pada aplikasi, termasuk melakukan reviu kode sumber apabila diperlukan; e) Komitmen dan *service level agreement* (SLA) terkait penyelesaian jika terdapat *error, bug,* atau permasalahan dan insiden terkait keamanan aplikasi; f) Jaminan tidak terdapat *malicious code* dan *backdoor*; g) Perjanjian kerahasiaan.
PENGEMBANGAN	
1	Penyimpanan dan pengelolaan tiap versi kode sumber secara aman (*security repository & version control*).
2	Pemisahan lingkungan pengembangan dari lingkungan produksi.
3	Memastikan seluruh proses pengujian terdokumentasi dengan baik.
IMPLEMENTASI DAN OPERASIONAL	
1	Identifikasi standar konfigurasi keamanan dan penguatan keamanan (*security hardening*), sekurang-kurangnya meliputi: a) Konfigurasi penguatan keamanan sistem operasi; b) Perubahan akun, *password*, dan konfigurasi *default*; c) Penonaktifan fungsi *debug*; d) Penyesuaian dan pembatasan hak akses sesuai kebutuhan lingkungan produksi; e) Penghapusan informasi sensitif pada kode sumber dan konfigurasi (*hardcoded & plain text sensitive information*); f) Penghapusan dan/atau penyesuaian akun, konfigurasi, dan data yang dihasilkan pada tahap pengembangan.
PEMELIHARAAN DAN PEMANTAUAN	
1	Penerapan dan pemantauan *audit log* yang mencatat informasi dan kejadian yang terkait dengan keamanan aplikasi, yang sekurang-kurangnya meliputi: a) Waktu, sumber, dan tujuan; b) Ancaman dan/atau kejadian keamanan yang berasal dari internal maupun eksternal; c) Aktivitas-aktivitas anomali di luar kondisi normal operasional.
2	Peninjauan ulang secara berkala terhadap aktivitas pengguna, khususnya pengguna dengan hak akses administratif (administrator/*super user*).

3	Pemantauan terhadap kerentanan pada komponen perangkat lunak dan aplikasi serta tindak lanjutnya (*patching*).

4. Audit Keamanan Aplikasi

PERENCANAAN	
1	Kebijakan tentang keamanan dalam perencanaan, pengembangan, implementasi, dan operasional, serta pemantauan dan pemeliharaan aplikasi yang terdokumentasi.
2	Identifikasi, penetapan peran, tanggung jawab, dan kewenangan dari pihak-pihak yang terkait dengan keamanan aplikasi.
3	Identifikasi standar kebutuhan dan dan persyaratan minimum keamanan aplikasi, meliputi: a) Kebutuhan kerahasiaan dan privasi; b) Kebutuhan integritas; c) Kebutuhan ketersediaan dan kontinuitas; d) Kebutuhan otentikasi; e) Kebutuhan otorisasi; f) Kebutuhan akuntabilitas dan non-repudiation; g) Kebutuhan peraturan, regulasi hukum dan perundang-undangan yang berlaku.
4	Identifikasi kendali keamanan tambahan, jika aplikasi dikembangkan oleh pihak ketiga, meliputi: a) Hak kekayaan intelektual, kepemilikan aplikasi, dan kode sumber asli; b) Penyimpanan kode sumber asli berdasarkan hak kepemilikan; c) Kualifikasi kapabilitas personil terkait keamanan aplikasi. d) Komitmen dan *service level agreement* (SLA) terkait penyelesaian jika terdapat *error, bug*, atau permasalahan dan insiden terkait keamanan aplikasi. e) Jaminan tidak terdapat *malicious code* dan *backdoor.* f) Perjanjian kerahasiaan.
PENGEMBANGAN	
1	Penyimpangan dan pengelolaan tiap versi kode sumber secara aman (*secure repository & version control*).
2	Pemisahan lingkungan pengembangan dari lingkungan produksi.
3	Memastikan seluruh proses pengujian terdokumentasi dengan baik.
IMPELENTASI DAN OPERASIONAL	
1	Identifikasi standar konfigurasi keamanan dan penguatan keamanan (*security hardening*) meliputi: a) Konfigurasi penguatan keamanan sistem operasi; b) Perubahan akun password dan konfigurasi *default*;

	c) Penonaktifan fungsi *debug*; d) Penyesuaian dan pembatasan hak akses sesuai kebutuhan lingkungan produksi; e) Penghapusan informasi sensitif pada kode sumber dan konfigurasi (*hardcoded & plain text sensitive information*); f) Penghapusan dan/atau penyesuaian akun, konfigurasi, dan data yang dihasilkan pada tahap pengembangan.
PEMELIHARAAN DAN PEMANTAUAN	
1	Penerapan dan pemantauan *audit log* yang mencatat informasi dan kejadian yang terkait dengan kemanan aplikasi, yang sekurang-kurangnya meliputi: a) Waktu, sumber, dan tujuan; b) Ancaman dan/atau kejadian keamanan yang berasal dari internal maupun eksternal; c) Aktivitas-aktivitas anomali di luar normal operasional.
2	Peninjauan ulang secara berkala terhadap aktivitas pengguna, khususnya pengguna dengan hak akses administratif (administrator/ *super user*).
3	Pemantauan terhadap kerentanan pada komponen perangkat lunak dan aplikasi serta tindak lanjutnya (*patching*).

BUPATI KOTAWARINGIN TIMUR,

HALIKINNOR