



BUPATI SUKOHARJO
PROVINSI JAWA TENGAH

KEPUTUSAN BUPATI SUKOHARJO
NOMOR : 500.12.6/667 TAHUN 2024

TENTANG

PETUNJUK TEKNIS AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BUPATI SUKOHARJO,

- Menimbang : a. bahwa untuk menjamin kualitas penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Sukoharjo, perlu dilaksanakan Audit Internal Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Petunjuk Teknis Audit Internal Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, dan huruf b, perlu menetapkan Keputusan Bupati;
- Mengingat : 1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah sebagaimana telah diubah dengan Undang-Undang Nomor 9 Tahun 1965 tentang Pembentukan Daerah Tingkat II Batang dengan mengubah Undang-Undang No. 13 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam Lingkungan Propinsi Jawa Tengah (Lembaran Negara Tahun 1965 Nomor 52, Tambahan Lembaran Negara Nomor 2757);
2. 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 Republik Indonesia Nomor 6856);
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

f

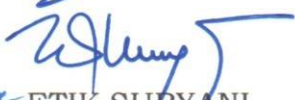
4. Peraturan Badan Riset Dan Inovasi Nasional Nomor 1 Tahun 2024 tentang Standar Dan Tata Cara Pelaksanaan Audit Infrastruktur dan Audit Aplikasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2024 Nomor 99);
5. Peraturan Daerah Kabupaten Sukoharjo Nomor 2 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Daerah Kabupaten Sukoharjo Tahun 2022 Nomor 2, Tambahan Lembaran Daerah Kabupaten Sukoharjo Nomor 303);
6. Peraturan Bupati Sukoharjo Nomor 59 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Sukoharjo Tahun 2022 Nomor 59);
7. Peraturan Bupati Sukoharjo Nomor 34 Tahun 2022 tentang Peta Rencana Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Sukoharjo Tahun 2022 Nomor 34) sebagaimana telah diubah dengan Peraturan Bupati Nomor 24 Tahun 2023 tentang Perubahan Atas Peraturan Bupati Nomor 34 Tahun 2022 tentang Peta Rencana Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Sukoharjo Tahun 2023 Nomor 24);

MEMUTUSKAN:

- Menetapkan :
- KESATU : Petunjuk Teknis Audit Internal Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik, sebagaimana tercantum dalam Lampiran Keputusan ini.
- KEDUA : Audit Internal Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik sebagaimana dimaksud Diktum KESATU terdiri atas:
- a. audit internal infrastruktur Sistem Pemerintahan Berbasis Elektronik;
 - b. audit internal aplikasi Sistem Pemerintahan Berbasis Elektronik; dan
 - c. audit internal keamanan Sistem Pemerintahan Berbasis Elektronik.

KETIGA : Keputusan Bupati ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Sukoharjo
pada tanggal 19 Juli 2024

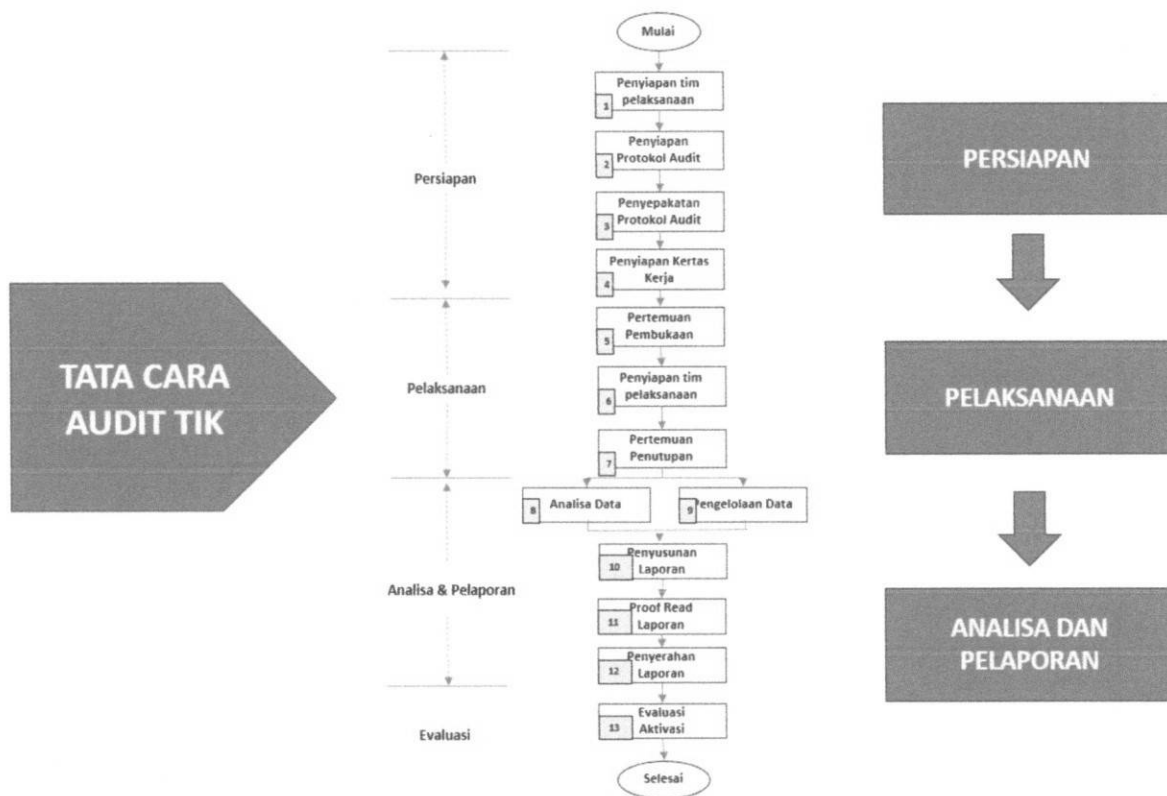
BUPATI SUKOHARJO, 

ETIK SURYANI

TEMBUSAN : Keputusan ini dikirim
kepada Yth.:

1. Ketua Dewan Perwakilan Rakyat Daerah Kabupaten Sukoharjo;
 2. Sekretaris Daerah Kabupaten Sukoharjo di Sukoharjo;
 3. Asisten Administrasi Umum Sekretaris Daerah Kabupaten Sukoharjo di Sukoharjo;
 4. Kepala Badan/Dinas/Bagian di Lingkungan Pemerintah Kabupaten Sukoharjo;
 5. Camat di Lingkungan Pemerintah Kabupaten Sukoharjo;
-

Lampiran : Keputusan Bupati Sukoharjo
Nomor : 500.12.6/667 TAHUN 2024
Tanggal : 19 Juli 2024

PETUNJUK TEKNIS AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK



I. STANDAR PELAKSANAAN AUDIT SPBE

Objek Audit TIK terdiri dari:

- infrastruktur SPBE yang terdiri dari Pusat Data, Jaringan Intra Pemerintah Daerah dan Sistem Penghubung Layanan Pemerintah Daerah;
- aplikasi SPBE Pemerintah Daerah, yang merupakan aplikasi khusus yang dikembangkan, dikelola dan/atau digunakan oleh Perangkat Daerah guna mendukung uraian tugas pokok dan fungsi serta memenuhi kebutuhan khusus Perangkat Daerah; dan
- keamanan infrastruktur dan keamanan aplikasi SPBE Pemerintah Daerah yang terkait pada huruf a dan huruf b.

Audit Teknologi Informasi dan Komunikasi meliputi pemeriksaan hal pokok teknis pada:

- penerapan tata kelola dan manajemen teknologi informasi dan komunikasi;
- fungsionalitas teknologi informasi dan komunikasi;
- kinerja teknologi informasi dan komunikasi yang dihasilkan; dan
- aspek teknologi informasi dan komunikasi lainnya.

Audit internal TIK dilaksanakan oleh tim auditor internal TIK Pemerintah Daerah yang mempunyai kompetensi teknis sesuai objek audit dan lingkup audit dan

6

ditetapkan oleh Sekretaris Daerah selaku Koordinator SPBE Pemerintah Daerah. Audit internal TIK dapat dilakukan dengan bantuan tenaga ahli audit TIK yang tersertifikasi atau lembaga audit TIK yang terakreditasi, dengan :

- a. memastikan bahwa tenaga ahli yang digunakan mempunyai kompetensi,
- b. kualifikasi profesi, pengalaman yang relevan, dan independensi; dan
- c. melakukan evaluasi terhadap hasil kerja tenaga ahli yang digunakan dan menyimpulkan tingkatan ketergunaannya.

II. PANDUAN TEKNIS AUDIT TIK

II.1 Tata Cara Pelaksanaan Audit

Pelaksanaan Audit SPBE terbagi dalam tiga kelompok tahapan, yaitu:

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

Tata laksana dalam tiga tahapan diatas sebagai berikut:

1. Penyiapan tim pelaksana meliputi penetapan personil tim audit.
2. Quick Assessment dilakukan untuk mengenali obyek audit dengan mengidentifikasi isu terkini (current issue), lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, proses bisnis dari organisasi, atau bagian yang diaudit, teknologi produk (bila relevan), teknologi proses (bila relevan), pengguna produk (bisa relevan)
3. Penyiapan protocol audit
Penyiapan protocol audit dimulai dengan komunikasi dengan auditee untuk menjelaskan secara garis besar tentang audit TIK. Tim auditor menindaklanjuti dengan menyusun protokol audit yang berisi detail instrumen audit, meliputi tujuan, lingkup, kriteria, acuan, metode pengumpulan data, metoda Analisa, perkiraan jadwal pelaksanaan, Daftar data, pertanyaan dan pengujian, Formulir untuk mencatat data, jawaban, hasil observasi dan hasil pengujian;
4. Penyeputusan protocol audit.
Komunikasi lanjutan dengan auditee dilakukan untuk menyepakati protocol yang disusun. Auditee dapat memberi masukan untuk memperbaiki protocol dan menunjuk personil di pihak auditee yang akan mendampingi auditor dalam pelaksanaan lapangan. Dokumen protocol ditandatangani oleh penanggung jawab tim auditor dan penanggung jawab tim auditee.
5. Penyiapan kertas kerja dan penyiapan audit tools
Setelah protocol audit disepakati, tim auditor menyiapkan secara rinci form-form yang diperlukan. Form tersebut dianggap sebagai kerja kerja formal dalam pengumpulan data
6. Melakukan pertemuan pembukaan dengan auditee
Pelaksanaan lapangan diawali dengan pertemuan pembukaan yang memaparkan rincian pelaksanaan lapangan audit aplikasi TIK dengan diawali dengan tata cara pelaksanaan audit melalui
7. Melaksanakan audit lapangan, melalui:
 - 1) Penelaahan dokumen;
 - 2) Wawancara;
 - 3) Observasi lapangan;
 - 4) Pengujian; dan
 - 5) Verifikasi bukti. Auditor dapat meminta data atau informasi guna keperluan pelaksanaan tugas, baik dalam bentuk salinan cetak maupun salinan lunak termasuk basis data dari Aplikasi SPBE
8. Melakukan analisis bukti;

9. Memberikan rekomendasi perbaikan untuk mengatasi temuan audit TIK. Temuan Audit TIK merupakan keadaan dimana fakta status penyelenggaraan SPBE Auditee tidak sesuai dengan ketentuan peraturan perundang-undangan serta standar penyelenggaraan SPBE.
10. Melakukan pertemuan penutupan dengan auditee;
11. Penyusunan laporan;
12. Proof-read laporan (memeriksa kembali laporan hasil audit);
13. Penyerahan laporan;
14. Evaluasi aktivitas

II.2 Pedoman Teknis Audit Infrastruktur SPBE

- a. Audit TIK Infrastruktur SPBE dengan obyek pusat data, jaringan infra dan sistem penghubung layanan, dilakukan pada aspek:
 1. Tata kelola infrastruktur SPBE, yang meliputi evaluasi, pengarahannya, dan pemantauan;
 2. Manajemen Infrastruktur SPBE, yang meliputi
 - a) Manajemen keamanan,
 - b) Manajemen risiko,
 - c) Manajemen asset,
 - d) Manajemen pengetahuan,
 - e) Manajemen sumber daya manusia (SDM),
 - f) Manajemen layanan, Manajemen perubahan, dan
 - g) Manajemen data;
 3. Fungsionalitas dan kinerja operasional dan pemeliharaan Infrastruktur SPBE, yang meliputi perencanaan, pengembangan, pengoperasian, dan pemeliharaan infrastruktur SPBE; dan
 4. Tingkat kepatuhan terhadap regulasi.
- b. Auditor melakukan pemeriksaan terhadap Infrastruktur SPBE untuk memastikan bahwa:
 1. Perubahan teknologi, ketentuan hukum, dan regulasi dipantau;
 2. Strategi Infrastruktur SPBE dan rencana Infrastruktur SPBE sudah selaras dengan kebutuhan Perangkat Daerah;
 3. Standar teknologi sudah ditetapkan dan diimplementasikan; dan
 4. Rekomendasi arsitektur Infrastruktur SPBE sudah dilaksanakan.
 5. Rencana pengadaan Infrastruktur SPBE sudah mempertimbangkan faktor risiko, biaya, manfaat, keamanan, dan kesesuaian teknis dengan Infrastruktur SPBE lainnya.
 6. Pengadaan Infrastruktur SPBE sesuai dengan rencana.
 7. Aset SPBE sudah diidentifikasi, ditentukan pemilik atau penanggung jawabnya, dan dicatat agar dapat dilindungi secara tepat.
 8. Penghapusan aset SPBE sudah dilakukan dengan tepat sehingga aset aman untuk dihapus dan/atau dimusnahkan.
 9. Kapasitas Infrastruktur SPBE sudah direncanakan dengan baik, dipantau, dianalisis dan dievaluasi penggunaannya.
 10. Insiden terkait Infrastruktur SPBE dicatat dan ditangani dengan baik sesuai dengan kesepakatan tingkat layanan.
 11. Pemeliharaan Infrastruktur SPBE telah dilakukan secara reguler sesuai dengan petunjuk penggunaannya; dan
 12. Setiap pegawai/petugas pengelola fasilitas, Infrastruktur SPBE harus memiliki kompetensi yang sesuai dengan bidang tugasnya.
- c. Audit dapat difokuskan pada penilaian fungsionalitas dan kinerja infrastruktur SPBE.
- d. Auditor harus melakukan pemeriksaan terhadap penyediaan layanan infrastruktur SPBE oleh pihak eksternal untuk memastikan bahwa :
 1. Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;

2. Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
 3. Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan
 4. Perjanjian Kerahasiaan (Non Disclosure Agreement) telah ditandatangani oleh pihak eksternal.
- e. Panduan teknis dan kriteria penilaian pada audit infrastruktur SPBE dapat ditetapkan lebih lanjut oleh APIP, sesuai ketentuan peraturan perundang-undangan.

II.3 Pedoman Teknis Audit Aplikasi SPBE

a. Audit Aplikasi SPBE dilakukan pada aspek:

1. Penerapan tata kelola Aplikasi SPBE yang meliputi evaluasi, pengarahan, dan pemantauan;
2. Penerapan manajemen Aplikasi SPBE, yang meliputi
 - a) Manajemen keamanan,
 - b) Manajemen risiko,
 - c) Manajemen asset,
 - d) Manajemen pengetahuan,
 - e) Manajemen sumber daya manusia,
 - f) Manajemen layanan,
 - g) Manajemen perubahan, dan
 - h) Manajemen data;
3. Fungsionalitas dan Kinerja Aplikasi SPBE yang meliputi perencanaan, pengembangan, pengoperasian, dan pemeliharaan aplikasi SPBE; dan
4. Tingkat kepatuhan terhadap regulasi.

b. Auditor harus melakukan pemeriksaan terhadap Arsitektur Aplikasi SPBE paling sedikit untuk memastikan bahwa:

1. Aplikasi direncanakan dalam suatu dokumen spesifikasi kemampuan aplikasi (Software Requirements Specifications) dengan mengacu kepada arsitektur SPBE Nasional, arsitektur SPBE Pemerintah Daerah, dengan mempertimbangkan kebutuhan, peluang dan proses bisnis;
2. Perubahan kebutuhan dan proses bisnis dipantau;
3. Standar pembangunan dan pengembangan Aplikasi SPBE sudah ditetapkan dan diimplementasikan;
4. Rekomendasi arsitektur Aplikasi SPBE sudah dilaksanakan.
5. Aplikasi SPBE sudah dibangun dan dikembangkan sesuai rencana dengan metodologi pembangunan dan pengembangan yang ada;
6. Rancangan Aplikasi SPBE sudah mempertimbangkan kebutuhan keamanan dan ketersediaan;
7. Aplikasi SPBE memiliki dokumentasi pembangunan dan pengembangan Aplikasi SPBE yang dibutuhkan;
8. Aplikasi SPBE sudah diujicobakan sebelum dioperasikan sesuai dengan kebutuhannya. Uji coba terhadap aplikasi harus terdokumentasi.
9. Pengendalian akses ke kode sumber (source code) Aplikasi SPBE sudah dilakukan;
10. Pelatihan kepada pengguna dan pegawai/petugas pengelola Aplikasi SPBE telah dilakukan;
11. Tinjauan pasca implementasi telah dilakukan ketika selesai implementasi Aplikasi SPBE.
12. Kapasitas Aplikasi SPBE sudah direncanakan dengan baik, dipantau, dianalisis dan dievaluasi penggunaannya;
13. Insiden terkait Aplikasi SPBE dicatat dan ditangani dengan baik sesuai dengan kesepakatan tingkat layanan;

14. Pengoperasian dan pemeliharaan Aplikasi SPBE telah dilakukan secara rutin sesuai dengan pedoman; dan
 15. Setiap pegawai/petugas pengelola Aplikasi SPBE harus mempunyai kompetensi yang sesuai dengan bidang tugasnya.
- c. Auditor harus melakukan pemeriksaan terhadap penyediaan layanan pengembangan dan/atau pemeliharaan aplikasi SPBE oleh pihak ketiga, paling sedikit untuk memastikan bahwa:
1. Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;
 2. Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
 3. Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan
 4. Perjanjian Kerahasiaan (Non Disclosure Agreement) telah ditandatangani oleh pihak eksternal.
- d. Panduan teknis dan kriteria penilaian pada audit aplikasi SPBE dapat ditetapkan lebih lanjut oleh APIP, sesuai ketentuan peraturan perundang-undangan.

II.4 Pedoman Teknis Audit Keamanan SPBE

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

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

II.5 Pembiayaan Audit TIK

- a. Pembiayaan untuk pelaksanaan Audit TIK dapat ditanggung oleh:
 1. APIP;
 2. Perangkat Daerah yang membidangi urusan komunikasi dan informatika; dan/atau
 3. Auditee yang mengusulkan kegiatan audit TIK.
- b. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas proses bisnis.

- c. Mekanisme penganggaran audit TIK dapat dilakukan melalui perjanjian kerja dengan pihak ketiga atau swakelola yang disesuaikan dengan ketentuan peraturan perundang-undangan.

BUPATI SUKOHARJO, P

ETIK SURYANI