BUPATI LAMPUNG TENGAH
PROVINSI LAMPUNG

PERATURAN BUPATI LAMPUNG TENGAH
NOMOR 25 TAHUN 2022

TENTANG

PEDOMAN AUDIT TATA KELOLA TEKNOLOGI INFORMASI *(INFORMATION TECHNOLOGY GOVERNANCE)*

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI LAMPUNG TENGAH,

Menimbang :

a. bahwa penyelenggaraan pemerintahan dalam rangka pelayanan publik memerlukan *good governance* yang akan menjamin transparansi, akuntabilitas, efisiensi, dan efektivitas penyelenggaraan pemerintahan;

b. bahwa untuk pemanfaatan teknologi informasi dan komunikasi oleh institusi pemerintahan telah semakin meningkat, sehingga untuk memastikan pemanfaatan teknologi informasi dan komunikasi tersebut benar-benar mendukung tujuan penyelenggaraan pemerintahan daerah, maka harus memperhatikan efisiensi penggunaan sumber daya dan pengelolaan risiko;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Pedoman Audit Tata Kelola Teknologi Informasi *(Information Technology Governance)*.

Mengingat :

1. Undang-undang Nomor 28 Tahun 1959 tentang Penetapan Undang-undang Darurat Nomor 4 Tahun 1956 tentang Pembentukan Daerah Otonom Kabupaten-Kabupaten dalam Lingkungan Provinsi Sumatera Selatan (Lembaran Negara Republik Indonesia Tahun 1956 Nomor 55, Tambahan Lembaran Negara Republik Indonesia Nomor 1091) sebagai Undang-undang (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 1821);

2. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia

Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881) sebagaimana telah diubah dengan Undang-undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);

3. 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);
4. Undang-undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nornor 5038);
5. 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 dengan Undang-Undang Nomor 19 Tahun 2016 (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
6. 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 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Menteri Komunikasi dan Informatika Nomor: 41/PER/M.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;
10. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
11. Peraturan Menteri Pemberdayaan Aparatur Negara dan

Reformasi Birokrasi Nomor 5 Tahun 2018 tentang Pedoman Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 154);

12. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 19 Tahun 2018 tentang Penyusunan Peta Proses Bisnis Instansi Pemerintah (Berita Negara Republik Indonesia Tahun 2018 Nomor 411);
13. Peraturan Daerah Kabupaten Lampung Tengah Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Lampung Tengah (Lembaran Daerah Kabupaten Lampung Tengah Tahun 2016 Nomor 09, Tambahan Lembaran Daerah Kabupaten Lampung Tengah Nomor 6) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Lampung Tengah Nomor 10 Tahun 2021 (Lembaran Daerah Kabupaten Lampung Tengah Tahun 2021, Tambahan Lembaran Daerah Kabupaten Lampung Tengah Nomor 57);
14. Peraturan Daerah Kabupaten Lampung Tengah Nomor 08 Tahun 2020 tentang Sistem Pemerintahan Berbasis Elekronik dalam Penyelenggaraan Pemerintahan Daerah di Kabupaten Lampung Tengah (Lembaran Daerah Kabupaten Lampung Tengah Tahun 2020 Nomor 08, Tambahan Lembaran Daerah Kabupaten Lampung Tengah Nomor 49).

MEMUTUSKAN:

Menetapkan : **PERATURAN BUPATI TENTANG PEDOMAN AUDIT TATA KELOLA TEKNOLOGI INFORMASI *(INFORMATION TECHNOLOGY GOVERNANCE)***

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Lampung Tengah.
2. Bupati adalah Bupati Lampung Tengah.
3. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi

kewenangan daerah otonom.

4. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam Penyelenggaraan urusan Pemerintahan yang menjadi kewenangan daerah.
5. Dinas adalah Dinas Komunikasi, Informatika dan Statistik Kabupaten Lampung Tengah.
6. Audit adalah proses identifikasi masalah, analisis dan evaluasi bukti yang dilakukan secara independent, obyektif dan professional berdasarkan standar audit untuk menilai kebenaran, kecermatan, kredibilitas, efektifitas, efesiensi dan keandalan informasi pelaksanaan tugas dan fungsi instansi pemerintah.
7. Audit Tata Kelola Teknologi Informasi *(Information Technology Governance)* yang selanjutnya disebut Audit Tata Kelola Teknologi Informasi *(IT Governance)* adalah audit yang bertujuan untuk memeriksa apakah tata kelola sumber data teknologi informasi (termasuk didalamnya manajemen organisasi dan pimpinan) dapat mendukung dan sejalan dengan strategi bisnis.

BAB II
MAKSUD DAN TUJUAN

Pasal 2

(1) Maksud disusunnya Peraturan Bupati ini adalah untuk menjamin kelancaran dan kesamaan tata cara pelaksanaan audit tata kelola Teknologi Informasi *(IT Governance)* serta penilaian atas ketercapaian efektifitas dan efesiensi Tata Kelola Teknologi Informasi.

(2) Tujuan disusunnya Peraturan Bupati ini adalah sebagai pedoman bagi Pegawai Negeri Sipil yang ditugaskan untuk melakukan Audit Tata Kelola Teknologi Informasi *(IT Governance)* dengan memperhatikan norma, standar dan prosedur yang ditetapkan.

BAB III
PELAKSANAAN AUDIT TATA KELOLA TEKNOLOGI INFORMASI *(INFORMATION TECHNOLOGY GOVERNANCE)*

Pasal 3

Pedoman Audit Tata Kelola Teknologi Informasi *(IT Governance)* tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dari peraturan Bupati ini.

BAB IV

PEMBIAYAAN

Pasal 4

Pembiayaan yang diperlukan dalam rangka pelaksanaan Audit Tata Kelola Teknologi Informasi *(IT Governance)* dibebankan pada Anggaran Pendapatan dan Belanja Daerah.

BAB V
KETENTUAN PENUTUP

Pasal 5

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang yang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Lampung Tengah.

Ditetapkan di Gunung Sugih
pada tanggal 4 april 2022

BUPATI LAMPUNG TENGAH,

Ttd

MUSA AHMAD

Diundangkan di Gunung Sugih
pada tanggal 4 april 2022

SEKRETARIS DAERAH
KABUPATEN LAMPUNG TENGAH,

Ttd

NIRLAN

BERITA DAERAH KABUPATEN LAMPUNG TENGAH TAHUN 2022 NOMOR **25**

LAMPIRAN PERATURAN BUPATI LAMPUNG TENGAH
NOMOR : TAHUN 2022

TENTANG : PEDOMAN AUDIT TATA KELOLA TEKNOLOGI INFORMASI *(INFORMATION TECHNOLOGY GOVERNANCE)*

PEDOMAN AUDIT TEKNOLOGI INFORMASI
(INFORMATION TECHNOLOGY GOVERNANCE)

I. Pedoman Umum Audit Teknologi Informasi *(Information Technology Governance):*
   a. Audit Teknologi Informasi bertujuan untuk memberikan rekomendasi perbaikan terhadap kelemahan pengendalian Informasi Teknologi baik yang bersifat umum maupun aplikasi.
   b. Auditor harus menjunjung tinggi kode etik (etika) dalam melaksanakan tugas, yaitu sebagai berikut:
      1. Integritas:
         a. Bekerja dengan jujur, tekun, dan bertanggung jawab;
         b. Taat terhadap peraturan dan membuat pengungkapan yang sesuai dengan ketentuan peraturan perundang-undangan;
         c. Tidak melakukan kegiatan yang ilegal; dan
         d. Menghormati dan berperan dalam mendukung tujuan Kementerian.
      2. Objektif:
         a. Tidak ikut berperan dalam kegiatan yang dapat mempengaruhi objektivitas pelaksanaan tugas Audit Teknologi Informasi;
         b. Tidak menerima apapun yang dapat mempengaruhi pelaksanaan tugas Audit Teknologi Informasi dan bekerja sesuai keahliannya; dan
         c. Mengungkapkan fakta sebagaimana yang ditemukan dalam pelaksanaan tugas Audit Teknologi Informasi.
      3. Menjaga kerahasiaan:
         a. Berhati-hati dalam penggunaan data atau informasi dan melindungi data atau informasi yang diperoleh dalam pelaksanaan tugas Audit Teknologi Informasi; dan
         b. Tidak menggunakan data atau informasi yang diperoleh untuk kepentingan pribadi ataupun bertentangan dengan hukum.
      4. Memiliki kompetensi
         a. Memiliki pengetahuan yang memadai;
         b. Melaksanakan tugas Audit Informasi Teknologi sesuai dengan ketentuan peraturan perundang-undangan; dan
         c. Berusaha terus menerus meningkatkan kemampuan untuk meningkatkan kualitas Audit Informasi Teknologi.
   c. Kegiatan Audit Informasi Teknologi dilakukan berdasarkan uraian yang disusun di dalam surat penugasan kerja Audit Informasi Teknologi. Surat penugasan kerja Audit Informasi Teknologi

berisikan antara lain:

1. Tujuan Audit Informasi Teknologi;
2. Cakupan Audit Informasi Teknologi;
3. Wewenang auditor;
4. Kewajiban auditor;
5. Tanggung jawab auditor; dan
6. Tata pelaporan hasil Audit Informasi Teknologi.

d. Dalam semua hal terkait kegiatan Audit Informasi Teknologi, auditor dan unit kerja yang menyelenggarakan fungsi pengawasan intern harus berlaku independen dan objektif. Auditor bukan bagian dari anggota tim yang mengerjakan atau menjalani tugas dari fungsi yang akan diaudit.
e. Auditor harus menyusun perencanaan dan program audit teknologi informasi dan komunikasi berdasarkan pendekatan risiko (*risk approach*). Hasil penilaian risiko digunakan untuk mengatur prioritas dan pengalokasian sumber daya audit.
f. Auditor dapat meminta bantuan tenaga ahli dalam pelaksanaan Audit Informasi Teknologi. Hal-hal yang harus dilakukan jika menggunakan bantuan tenaga ahli lainnya antara lain:
    1. Memastikan bahwa tenaga ahli yang digunakan mempunyai kompetensi, kualifikasi profesi, pengalaman yang relevan, dan independensi; dan
    2. Melakukan evaluasi terhadap hasil kerja tenaga ahli yang digunakan dan menyimpulkan tingkatan ketergunaannya.

II. Metodologi Audit Informasi Teknologi

a. Perencanaan Audit Informasi Teknologi
    1. Audit Informasi Teknologi harus direncanakan dengan mempertimbangkan hasil penilaian risiko SPBE yang dilakukan. Dalam melakukan penilaian risiko, Audit Informasi Teknologi paling sedikit melakukan beberapa hal sebagai berikut:
        a) Mengidentifikasi aset Informasi Teknologi yang berupa data, Aplikasi SPBE, sistem operasi, Infrastruktur SPBE, fasilitas, dan personil;
        b) Mengidentifikasi kegiatan dan proses bisnis yang menggunakan Informasi Teknologi; dan
        c) Mengidentifikasi tingkat dampak risiko SPBE dalam operasional layanan SPBE dan mempertimbangkan skala prioritas berdasarkan tingkat risiko.
    2. Rencana kerja Audit Informasi Teknologi harus disusun untuk setiap penugasan Audit Informasi Teknologi, yang paling sedikit mencakup:
        a) Tujuan Audit Informasi Teknologi, jadwal, jumlah auditor, dan pelaporan;
        b) Cakupan Audit Informasi Teknologi sesuai hasil penilaian risiko; dan
        c) Pembagian tugas dan tanggung jawab dari auditor.

3. Audit Informasi Teknologi dapat dilakukan oleh sebuah tim Audit Informasi Teknologi yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut:
    a) Pengawas Mutu, berperan melakukan monitoring dan evaluasi aktivitas Audit Informasi Teknologi untuk menjamin pelaksanaan Audit Informasi Teknologi sesuai dengan ketentuan peraturan perundangundangan;
    b) *Lead Auditor*, bertanggung jawab merencanakan Audit Informasi Teknologi, melaksanakan Audit Informasi Teknologi di lapangan, mengendalikan data dan melaporkan hasil Audit Informasi Teknologi;
    c) Auditor, bertugas membantu *Lead Auditor* dalam aktivitas Audit Informasi Teknologi;
    d) Asisten Auditor, bertugas membantu Auditor dalam aktivitas Audit Informasi Teknologi. Asisten Auditor harus sudah mengikuti sosialisasi
    Audit Informasi Teknologi;
    e) Teknisi, bertugas membantu Auditor dalam pengumpulan data lapangan; dan
    f) Narasumber, berperan memberi masukan yang berkaitan dengan isu, status industri dan teknologi, serta keilmuan yang relevan dengan lingkup yang diaudit.

    Dalam suatu Audit Informasi Teknologi, minimal terdiri dari seorang *Lead Auditor*.
4. Menyusun program Audit Informasi Teknologi sesuai dengan cakupan Audit Informasi Teknologi yang sudah ditetapkan dari hasil penilaian risiko SPBE. Auditor dapat mengalokasikan sumber daya yang lebih fokus pada area yang berisiko tinggi dan mempunyai skala kepentingan yang tinggi pada Layanan SPBE.
5. Auditor menyiapkan kertas kerja Audit Informasi Teknologi untuk mendokumentasikan pelaksanaan Audit Informasi Teknologi.
6. Auditor menetapkan populasi sampel yang akan diuji sesuai cakupan kendali.

b. Pelaksanaan Audit Informasi Teknologi
    1. Proses pelaksanaan Audit Informasi Teknologi mengacu pada program Audit Informasi Teknologi yang telah disusun pada tahap perencanaan dan seluruh hasil dari pelaksanaan Audit Informasi Teknologi harus dituangkan dalam dokumen kertas kerja Audit Informasi Teknologi.
    2. Dalam pelaksanaan kegiatan Audit Informasi Teknologi, auditor harus:
        a) Mampu menjamin tujuan Audit Informasi Teknologi tercapai sesuai dengan ketentuan peraturan perundang-undangan;
        b) Mengumpulkan bukti yang cukup, terpercaya, dan

relevan untuk mendukung temuannya; dan

c) Mendokumentasikan proses Audit Informasi Teknologi yang menjabarkan pelaksanaan Audit Informasi Teknologi dan bukti-bukti yang mendukung kesimpulannya.

3. Auditor melakukan pemeriksaan terhadap Infrastruktur SPBE, Aplikasi SPBE, dan Keamanan SPBE yang dikelola oleh Kementerian.
4. Pelaksanaan Audit Informasi Teknologi meliputi pemeriksaan hal pokok teknis pada:
   a) Penerapan tata kelola dan manajemen Informasi Teknologi;
   b) Fungsionalitas Informasi Teknologi;
   c) Kinerja Informasi Teknologi yang dihasilkan; dan
   d) Aspek Informasi Teknologi lainnya.
5. Memberikan rekomendasi perbaikan untuk mengatasi kekurangan dalam penyelenggaraan SPBE.
6. Auditor dapat meminta data atau informasi guna keperluan pelaksanaan tugas, baik dalam bentuk *hardcopy* maupun *softcopy* termasuk basis data dari Aplikasi SPBE.
7. Dalam pelaksanaan tugas, auditor Informasi Teknologi harus memperhatikan aspek kerahasiaan data dan informasi yang diperolehnya.

c. Pelaporan Audit Informasi Teknologi
   1. Seluruh hasil pemeriksaan dikonfirmasikan kepada *auditee* untuk memutuskan apakah kesimpulan hasil pemeriksaan, termasuk temuan yang diperoleh selama Audit Informasi Teknologi berlangsung dapat diterima oleh *auditee*.
   2. Auditor harus memberikan laporan hasil audit setelah konfirmasi dilakukan. Laporan ini harus berisikan antara lain:
      a) Tujuan Audit Informasi Teknologi;
      b) Cakupan Audit Informasi Teknologi;
      c) Periode pelaksanaan Audit Informasi Teknologi;
      d) Hasil pemeriksaan, kesimpulan, dan rekomendasi;
      e) Tanggapan *auditee* terhadap hasil Audit Informasi Teknologi;
      f) Batasan dan kendala yang ditemui selama proses Audit Informasi Teknologi;
      g) Tata cara pendistribusian laporan sesuai dengan surat penugasan.
   3. Laporan hasil Audit Informasi Teknologi harus disampaikan kepada Pimpinan atau pihak yang berkepentingan.

d. Pemantauan Tindak Lanjut Audit Informasi Teknologi
   1. Apabila temuan perlu ditindaklanjuti maka *auditee* harus memberikan komitmen dan target waktu penyelesaiannya.
   2. Auditor harus melakukan pemantauan atas temuan dan rekomendasi yang dilaporkan untuk memastikan langkah-langkah perbaikan sudah dilakukan oleh pimpinan unit organisasi.

3. Auditor harus memelihara dokumentasi atas hasil tindak lanjut tersebut.

III. Program Audit Informasi Teknologi

a. Cakupan Audit Informasi Teknologi

1. Cakupan Audit Informasi Teknologi di sini adalah:
   a) Audit Infrastruktur SPBE;
   b) Audit Aplikasi Khusus SPBE;
   c) Audit Keamanan SPBE; dan
   d) Audit Pengelolaan Informasi Teknologi oleh Pihak Eksternal.
2. Cakupan Audit Informasi Teknologi dapat dilakukan secara terpisah sesuai kebutuhan.

b. Audit Infrastruktur SPBE

1. Melakukan Audit Informasi Teknologi Infrastruktur SPBE terhadap:
   a) Arsitektur Infrastruktur SPBE;
   b) Peta Rencana Infrastruktur SPBE;
   c) Manajemen aset Informasi Teknologi; dan
   d) Kinerja operasional dan pemeliharaan Infrastruktur SPBE.
2. Auditor harus melakukan pemeriksaan terhadap Arsitektur Infrastruktur SPBE paling sedikit untuk memastikan bahwa:
   a) Perubahan teknologi, ketentuan hukum, dan regulasi dipantau;
   b) Strategi Infrastruktur SPBE dan rencana Infrastruktur SPBE sudah selaras dengan kebutuhan Kementerian;
   c) Standar teknologi sudah ditetapkan dan diimplementasikan; dan
   d) Rekomendasi arsitektur Infrastruktur SPBE sudah dilaksanakan.
3. Auditor harus melakukan pemeriksaan terhadap Peta Rencana Infrastruktur SPBE paling sedikit untuk memastikan bahwa:
   a) Peta Rencana Infrastruktur SPBE telah disusun berdasarkan analisa kesenjangan arsitektur Infrastruktur SPBE;
   b) Peta Rencana Infrastruktur SPBE disusun berdasarkan prioritas pengembangannya;
   c) Implementasi Peta Rencana SPBE; dan
   d) Peta Rencana Infrastruktur SPBE ditinjau secara berkala berdasarkan prioritasi kebutuhan, rencana anggaran, atau hasil evaluasi SPBE.
4. Auditor harus melakukan pemeriksaan terhadap Manajemen Aset Informasi Teknologi paling sedikit untuk memastikan bahwa:
   a) Rencana pengadaan Infrastruktur SPBE sudah mempertimbangkan faktor risiko, biaya, manfaat, keamanan, dan kesesuaian teknis dengan Infrastruktur SPBE lainnya.
   b) Pengadaan Infrastruktur SPBE sesuai dengan rencana.

c) Aset Informasi Teknologi sudah diidentifikasikan, ditentukan pemilik atau penanggung jawabnya, dan dicatat agar dapat dilindungi secara tepat.
d) Penghapusan aset Informasi Teknologi sudah dilakukan dengan tepat sehingga aset aman untuk dihapus dan/atau dimusnahkan.

5. Auditor harus melakukan pemeriksaan terhadap kinerja operasional dan pemeliharaan Infrastruktur SPBE paling sedikit untuk memastikan bahwa:
   a) Kapasitas Infrastruktur SPBE sudah direncanakan dengan baik, dipantau, dianalisis dan dievaluasi penggunaannya.
   b) Insiden terkait Infrastruktur SPBE dicatat dan ditangani dengan baik sesuai dengan kesepakatan tingkat layanan.
   c) Pemeliharaan Infrastruktur SPBE telah dilakukan secara reguler sesuai dengan petunjuk penggunaannya; dan
   d) Setiap petugas pengelola fasilitas, Infrastruktur SPBE harus memiliki kompetensi yang sesuai dengan bidang tugasnya.

c. Audit Aplikasi SPBE
1. Melakukan Audit Aplikasi SPBE terhadap:
   a) Arsitektur Aplikasi SPBE;
   b) Peta Rencana Aplikasi SPBE;
   c) Pembangunan dan pengembangan Aplikasi Khusus; dan
   d) Kinerja Layanan Aplikasi SPBE.
2. Auditor harus melakukan pemeriksaan terhadap Arsitektur Aplikasi SPBE paling sedikit untuk memastikan bahwa:
   a) Perubahan kebutuhan dan proses bisnis dipantau;
   b) Strategi Aplikasi SPBE dan rencana Aplikasi SPBE sudah selaras dengan kebutuhan Kementerian;
   c) Standar pembangunan dan pengembangan Aplikasi SPBE sudah ditetapkan dan diimplementasikan; dan
   d) Rekomendasi arsitektur Aplikasi SPBE sudah dilaksanakan.
3. Auditor harus melakukan pemeriksaan terhadap Peta Rencana Aplikasi SPBE paling sedikit untuk memastikan bahwa:
   a) Peta Rencana Aplikasi SPBE telah disusun berdasarkan analisa kesenjangan arsitektur Aplikasi SPBE;
   b) Peta Rencana Aplikasi SPBE disusun berdasarkan prioritas pengembangannya;
   c) Sejauh mana Peta Rencana Aplikasi SPBE sudah diimplementasikan; dan
   d) Peta Rencana Aplikasi SPBE ditinjau secara berkala berdasarkan prioritasi kebutuhan, rencana anggaran, atau hasil evaluasi SPBE.
4. Auditor harus melakukan pemeriksaan terhadap pembangunan dan pengembangan Aplikasi Khusus paling sedikit untuk memastikan bahwa:
   a) Aplikasi SPBE sudah dibangun dan dikembangkan sesuai

dengan metodologi pembangunan dan pengembangan yang ada;
b) Rancangan Aplikasi SPBE sudah mempertimbangkan kebutuhan keamanan dan ketersediaan;
c) Aplikasi SPBE sudah diujicobakan sebelum dioperasionalkan sesuai dengan kebutuhannya;
d) Aplikasi SPBE memiliki dokumentasi pembangunan dan pengembangan Aplikasi SPBE yang dibutuhkan;
e) Pengendalian akses ke kode sumber (*source code*) Aplikasi SPBE sudah dilakukan;
f) Pelatihan kepada pengguna dan tim pendukung Aplikasi SPBE telah dilakukan; dan
g) Tinjauan pasca implementasi telah dilakukan ketika selesai implementasi Aplikasi SPBE.

5. Auditor harus melakukan pemeriksaan terhadap kinerja layanan Aplikasi Khusus paling sedikit untuk memastikan bahwa:
a) Kapasitas Aplikasi SPBE sudah direncanakan dengan baik, dipantau, dianalisis dan dievaluasi penggunaannya;
b) Insiden terkait Aplikasi SPBE dicatat dan ditangani dengan baik sesuai dengan kesepakatan tingkat layanan;
c) Pemeliharaan Aplikasi SPBE telah dilakukan secara reguler sesuai dengan pedomannya; dan
d) Setiap petugas pengelola Aplikasi SPBE harus mempunyai kompetensi yang sesuai dengan bidang tugasnya.

d. Audit Keamanan SPBE

1. Melakukan Audit Keamanan SPBE terhadap:
a) Arsitektur Keamanan SPBE;
b) Peta Rencana Keamanan SPBE;
c) Manajemen keamanan informasi;
d) Keamanan Aplikasi Khusus; dan
e) Keamanan Infrastruktur SPBE.

2. Auditor harus melakukan pemeriksaan terhadap Arsitektur Keamanan SPBE paling sedikit untuk memastikan bahwa:
a) Perubahan ancaman, kerentanan, risiko, dan kendali SPBE dipantau;
b) Strategi Keamanan SPBE dan rencana Keamanan SPBE sudah selaras dengan kebutuhan Kementerian;
c) Standar keamanan informasi sudah ditetapkan dan diimplementasikan; dan
d) Rekomendasi arsitektur Keamanan SPBE sudah dilaksanakan.

3. Auditor harus melakukan pemeriksaan terhadap Peta Rencana Keamanan SPBE paling sedikit untuk memastikan bahwa:
a) Peta Rencana Keamanan SPBE telah disusun berdasarkan analisis risiko dan kesenjangan arsitektur Keamanan SPBE;
b) Peta Rencana Keamanan SPBE disusun berdasarkan

prioritas pengembangannya;
c) Sejauh mana Peta Rencana Keamanan SPBE sudah diimplementasikan; dan
d) Peta Rencana Keamanan SPBE ditinjau secara berkala berdasarkan kajian risiko, rencana anggaran, atau hasil evaluasi SPBE.

4. Auditor harus melakukan pemeriksaan terhadap manajemen keamanan informasi paling sedikit untuk memastikan bahwa:
   a) Kebijakan dan pedoman keamanan informasi sudah disusun dan disosialisasikan secara berkala;
   b) Dilakukan pelatihan peningkatan kepedulian (*awareness training*) keamanan informasi secara berkala;
   c) Pengelola dan pelaksana keamanan informasi sudah ditetapkan;
   d) Setiap sistem, Aplikasi SPBE, dan data telah ditentukan tingkat kritikalitasnya;
   e) Setiap sistem dan proses bisnis telah ditetapkan pemiliknya;
   f) Ada prosedur pengelolaan pengguna dan hak aksesnya untuk setiap pegawai dan pihak eksternal;
   g) Setiap pengguna sistem diberi hak akses sesuai dengan kebutuhan minimumnya dan disetujui oleh pemilik proses bisnis;
   h) Setiap pengguna sistem bisa diidentifikasi secara individual;
   i) Dilakukan tinjauan secara berkala terhadap pengguna dan hak aksesnya di setiap sistem;
   j) Dilakukan pemantauan keamanan sistem secara proaktif;
   k) Dilakukan pengujian keamanan sistem secara berkala;
   l) Insiden keamanan informasi ditangani secara efektif; dan
   m) Dilakukan perlindungan terhadap data yang bersifat rahasia.
5. Auditor harus melakukan pemeriksaan terhadap Keamanan Aplikasi Khusus untuk memastikan 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*.
6. Auditor harus melakukan pemeriksaan terhadap Keamanan Infrastruktur SPBE paling sedikit untuk memastikan bahwa:
   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 kritikal untuk dipantau.

e. Audit Pengelolaan Informasi Teknologi oleh Pihak Eksternal

Auditor harus melakukan pemeriksaan terhadap penyedia jasa Informasi Teknologi oleh pihak eksternal paling sedikit untuk memastikan bahwa:

a) Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;
b) Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
c) Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan
d) Perjanjian pengungkapan informasi tanpa izin (*Non Disclosure Agreement*) telah ditandatangani oleh pihak eksternal.

BUPATI LAMPUNG TENGAH,

MUSA AHMAD