BUPATI LEMBATA

PROVINSI NUSA TENGGARA TIMUR

PERATURAN BUPATI LEMBATA

NOMOR 63 TAHUN 2022

TENTANG

PEDOMAN AUDIT TATA KELOLA TEKNOLOGI INFORMASI DAN KOMUNIKASI DI LINGKUNGAN PEMERINTAHAN KABUPATEN LEMBATA

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI LEMBATA,

Menimbang : a. bahwa dalam rangka memastikan kehandalan dan keamanan sistem Teknologi Informasi dan Komunikasi di lingkungan Pemerintahan Kabupaten Lembata perlu dilakukan Audit Teknologi Informasu dan Komunikasi;

b. bahwa berdasarkan ketentuan Pasal 56 ayat (3), Pasal 57 ayat (4), dan Pasal 58 ayat (4) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), Ketentuan lebih lanjut mengenai standar dan tata cara pelaksanaan audit Infrastruktur Sistem Pemerintahan Berbasis Elektronik, Aplikasi Sistem Pemerintahan Berbasis Elektronik, dan Keamanan Sistem Pemerintahan Berbasis Elektronik diatur dengan Peraturan Lembaga Pemerintah Non Kementerian yang menyelenggarakan tugas pemerintahan di bidang Pengkajian dan Penerapan Teknologi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Pedoman Audit Tata Kelola Teknologi Informasi dan Komunikasi di Lingkungan Pemerintahan Kabupaten Lembata.

Mengingat : 1. Undang-Undang Nomor 52 Tahun 1999 tentang Pembentukan Kabupaten Lembata (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 180, Tambahan

Lembaran Negara Republik Indonesia Nomor 3901), sebagaimana telah diubah dengan Undang-Undang Nomor 12 Tahun 2000 tentang Perubahan Atas Undang-Undang Nomor 52 Tahun 1999 tentang Pembentukan Kabupaten Lembata (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 79, Tambahan Lembaran Negara Republik Indonesia Nomor 3967);

2. 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 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negraa Republik Indonesia Nomor 5952);
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 Nomor 5038);
5. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);

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 beberapa kali diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, 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 Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2018 Nomor 157);
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 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);

12. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
13. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
14. Peraturan Daerah Kabupaten Lembata Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Lembata (Lembaran Daerah Kabupaten Lembata Tahun 2016 Nomor 6) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Lembata Nomor 1 Tahun 2020 tentang Perubahan Atas Peraturan Daerah Kabupaten Lembata Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Lembata (Lembaran Daerah Kabupaten Lembatan Tahun 2020 Nomor 288);
15. Peraturan Bupati Lembata Nomor 27 Tahun 2022 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi dan Informatika (Berita Daerah Kabupaten Lembata Tahun 2022 Nomor 27);

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Lembata.
2. Pemerintah Daerah adalah Pemerintah Kabupaten Lembata.
3. Bupati adalah Bupati Lembata.
4. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Kepala Daerah dan Dewan Perwakilan Rakyat Daerah dalam

penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan daerah.

5. Dinas adalah Dinas Komunikasi dan Informatika Kabupaten Lembata.
6. Audit adalah proses identifikasi masalah, analisa dan evaluasi bukti yang dilakukan secara independent, objektif, dan professional berdasarkan standar audit untuk menilai kebenaran, kecermatan, kredibilitas, efektifitas, efesiensi, dan keandalan informasi pelaksanaan tugas dan fungsi instansi pemerintah.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah suatu sistem tata kelola pemerintahan yang memanfaatkan teknologi informasi dan komunikasi secara menyeluruh dan terpadu dalam pelaksanaan administrasi pemerintahan dan penyelenggaraan pelayanan publik pada Pemerintah Daerah.
8. Audit Teknologi Informasi dan Komunikasi yang selanjutnya disebut Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
9. 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.
10. 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.
11. Auditor adalah orang yang memiliki kompetensi pengetahuan dan keterampilan khusus dengan tugas utama melakukan evaluasi atas pengendalian sistem elektronik yang dapat dipertanggungjawabkan secara akademis maupun praktis.
12. Lembaga Pelaksana Audit TIK adalah lembaga yang melaksanakan Audit TIK.
13. Auditee adalah instansi pusat dan pemerintah daerah yang menjadi objek dari pelaksanaan Audit Infrastruktur SPBE dan Audit Aplikasi SPBE.

BAB II

MAKSUD DAN TUJUAN

Pasal 2

(1) Peraturan Bupati ini disusun untuk menjamin kelancaran dan kesamaan tata cara pelaksanaan Audit TIK serta penilaian atas ketercapaian efektifitas dan efisiensi Tata Kelola TIK.

(2) Peraturan Bupati ini disusun sebagai pedoman bagi Auditor Internal dalam melaksanakan Audit Tata Kelola TIK dengan memperhatikan norma, standar, dan prosedur yang ditetapkan.

BAB III

PELAKSANAAN AUDIT TIK

Pasal 3

Pedoman Audit TIK tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 4

(1) Auditor Internal untuk melakukan Audit TIK ditetapkan oleh Sekretaris Daerah sebagai Ketua Tim Pengarah SPBE.

(2) Auditee dalam proses audit internal ditetapkan oleh Sekretaris Daerah sebagai Ketua Tim Pengarah SPBE.

(3) Syarat Auditor Internal berkualifikasi Pranata Komputer atau Aparatur Sipil Negara yang kompeten di Bidang urusan Teknologi Informasi dan Komunikasi.

(4) Persiapan dan pelaksanaan Audit Internal TIK dilakukan oleh Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang komunikasi dan informatika berkerjasama dengan Perangkat Daerah penyelenggara pengawasan.

BAB IV

PEMBIAYAAN

Pasal 5

Pembiayaan yang diperlukan dalam rangka pelaksanaan Audit TIK dibebankan pada Anggaran Pendapatan dan Belanja Daerah.

BAB V

KETENTUAN PENUTUP

Pasal 6

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Lewoleba

pada tanggal 13 Juli 2022

PENJABAT BUPATI LEMBATA,

MARSIANUS JAWA

Diundangkan di Lewoleba

pada tanggal 13 Juli 2022

SEKRETARIS DAERAH KABUPATEN LEMBATA,

PASKALIS OLA TAPO BALI

BERITA DAERAH KABUPATEN LEMBATA TAHUN 2022 NOMOR 63

LAMPIRAN
PERATURAN BUPATI LEMBATA
NOMOR 63 TAHUN 2022
TENTANG
PEDOMAN AUDIT TATA KELOLA TEKNOLOGI INFORMASI DAN KOMUNIKASI DI LINGKUNGAN PEMERINTAHAN KABUPATEN LEMBATA

PEDOMAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK)

I. Pedoman Umum Audit TIK:
   a. Audit TIK bertujuan untuk memberikan rekomendasi perbaikan terhadap kelemahan pengendalian TIK baik yang bersifat umum maupun aplikasi;
   b. Auditor harus menjunjung tinggi kode etik dalam melaksanakan tugas, yaitu sebagai berikut:
      1. Integritas
         a. berkerja 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 TIK
         b. tidak menerima apapun yang dapat mempengaruhi pelaksanaan tugas Audit TIK dan berkerja sesuai keahliannya; dan
         c. mengungkapkan fakta sebagaimana yang ditemukan dalam pelaksanaan tugas Audit TIK.
      3. Menjaga kerahasiaan
         a. berhati-hati dalam penggunaan data atau informasi dan melindungi data atau informasi yang diperoleh dalam pelaksanaan tugas Audit TIK; dan
         a. 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 TIK sesuai dengan ketentuan peraturan perundang-undangan; dan
   c. berusaha terus menerus meningkatkan kemampuan untuk meningkatkan kualitas Audit TIK.

c. Kegiatan Audit TIK dilakukan berdasarkan uraian yang disusun di dalam surat penugasan kerja Audit TIK. Surat penugasan kerja Audit TIK berisikan antara lain:
   1. Tujuan Audit TIK;
   2. Cakupan TIK;
   3. Wewenang auditor;
   4. Kewajiban auditor;
   5. Tanggung jawab auditor; dan
   6. Tata pelaporan hasil Audit TIK.

d. Dalam semua hal terkait kegiatan Audit TIK, 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 TIK berdasarkan pendekatan risiko (*risk approach*). Hasil penilaian risiko digunakan untukmengatur prioritas dan pengalokasian sumber daya audit.

f. Auditor dapat meminta bantuan tenaga ahli dalam pelaksanaan Audit TIK. 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 TIK
   a. Perencanaan Audit TIK
      1. Audit TIK harus direncanakan dengan mempertimbangkan hasil penilaian risiko SPBE yang dilakukan. Dalam melakukan

penilaian risiko, Audit TIK paling sedikit melakukan beberapa hal sebagai berikut:

a) Mengidentifikasi aset TIK yang berupa data, Aplikasi SPBE, sistem operasi, Infrastruktur SPBE, fasilitas, dan personil;
b) Mengidentifikasi kegiatan dan proses bisnis yang menggunakan TIK; dan
c) Mengidentifikasi tingkat dampak risiko SPBE dalam operasional layanan SPBE dan mempertimbangkan skala prioritas berdasarkan tingkat risiko.

2. Rencana kerja Audit TIK harus disusun untuk setiap penugasan Audit TIK, yang paling sedikit mencakup:
   a) Tujuan Audit TIK, jadwal, jumlah auditor, dan pelaporan;
   b) Cakupan Audit TIK sesuai hasil penilaian risiko; dan
   c) Pembagian tugas dan tanggung jawab dari auditor.
3. Audit TIK dapat dilakukan oleh sebuah tim Audit TIK yang terdiri dari posisi-posisi berikut dengan uraian tugas dan tanggung jawab sebagai berikut:
   a) Pengawas Mutu, berperan melakukan monitoring dan evaluasi aktivitas Audit TIK untuk menjamin pelaksanaan Audit TIK sesuai dengan ketentuan peraturan perundangundangan;
   b) *Lead Auditor*, bertanggung jawab merencanakan Audit TIK, melaksanakan Audit TIK di lapangan, mengendalikan data dan melaporkan hasil Audit TIK;
   c) Auditor, bertugas membantu *Lead Auditor* dalam aktivitas Audit TIK;
   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 TIK, minimal terdiri dari seorang *Lead Auditor*.

4. Menyusun program Audit TIK sesuai dengan cakupan TIK 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 TIK untuk mendokumentasikan pelaksanaan Audit TIK.
6. Auditor menetapkan populasi sampel yang akan diuji sesuai cakupan kendali.

b. Pelaksanaan Audit TIK

1. Proses pelaksanaan Audit TIK mengacu pada program Audit TIK yang telah disusun pada tahap perencanaan dan seluruh hasil dari pelaksanaan Audit TIK harus dituangkan dalam dokumen kertas kerja Audit TIK.
2. Dalam pelaksanaan kegiatan TIK, auditor harus:
   a) Mampu menjamin tujuan Audit TIK tercapai sesuai dengan ketentuan peraturan perundangundangan;
   b) Mengumpulkan bukti yang cukup, terpercaya, dan relevan untuk mendukung temuannya; dan
   c) Mendokumentasikan proses Audit TIK yang menjabarkan pelaksanaan Audit TIK dan bukti-bukti yang mendukung kesimpulannya.
3. Auditor melakukan pemeriksaan terhadap Infrastruktur SPBE, Aplikasi SPBE, dan Keamanan SPBE yang dikelola oleh Pemerintah Daerah.
4. Pelaksanaan Audit TIK meliputi pemeriksaan hal pokok teknis pada:
   a) Penerapan tata kelola dan manajemen TIK
   b) Fungsionalitas TIK
   c) Kinerja TIK yang dihasilkan; dan
   d) Aspek TIK lainnya.
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 bisnis data dari aplikasi SPBE.

7. Dalam pelaksanaan tugas, auditor TIK harus memperhatikan aspek kerahasiaan data dan informasi yang diperolehnya.

c. Pelaporan Audit TIK

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

d. Pemantauan Tindak Lanjut Audit TIK

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

III. Program Audit TIK

a. Cakupan Audit TIK

1. Cakupan Audit TIK di sini adalah:
   a) Audit Infrastruktur SPBE Pemerintah Daerah;
   b) Audit Aplikasi Khusus SPBE Pemerintah Daerah;
   c) Audit Keamanan SPBE Pemerintah Daerah; dan
   d) Audit Pengelolaan TIK oleh Pihak Eksternal.

2. Cakupan Audit TIK dapat dilakukan secara terpisah sesuai kebutuhan

b. Audit Infrastruktur SPBE

1. Audit Infrastruktur SPBE dilakukan terhadap:
   a) Arsitektur Infrastruktur SPBE;
   b) Peta Rencana Infrastruktur SPBE;
   c) Manajemen aset TIK; 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 Infrastrukur 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 prioritas kebutuhan, rencana anggaran, atau hasil evaluasi SPBE.
4. Auditor harus melakukan pemeriksaan terhadap Manajemen Aset TIK 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 TIK sudah diidentifikasikan, ditentukan pemilik atau penanggung jawabnya, dan dicatat agar dapat dilindungi secara tepat; dan

d) Penghapusan aset TIK 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. Audit Aplikasi SPBE dilakukan 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. Audit Keamanan SPBE dilakukan 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 dengankebutuhan 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) Antar muka 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, *maluware*, dan lain-lain);

c) Pengendalian keamanan pada jaringan telah dilakukan; dan

d) Dilakukan identifikasi infrastruktur yang kritikal untuk dipantau.

e. Audit Pengelolaan TIK oleh Pihak Eksternal

Auditor harus melakukan pemeriksaan terhadap penyedia jasa TIK 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.

PENJABAT BUPATI LEMBATA,

MARSIANUS JAWA