LAMPIRAN III
PERATURAN MENTERI PEKERJAAN UMUM DAN PERUMAHAN RAKYAT REPUBLIK INDONESIA
NOMOR 27 TAHUN 2020
TENTANG
PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

AUDIT 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 (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 TIK;
   b) Tidak menerima apapun yang dapat mempengaruhi pelaksanaan tugas Audit TIK dan bekerja 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

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 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:
   a. Tujuan Audit TIK;
   b. Cakupan Audit TIK;
   c. Wewenang auditor;
   d. Kewajiban auditor;
   e. Tanggung jawab auditor; dan
   f. 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 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 TIK. Hal-hal yang harus dilakukan jika menggunakan bantuan tenaga ahli lainnya antara lain:
   a. Memastikan bahwa tenaga ahli yang digunakan mempunyai kompetensi, kualifikasi profesi, pengalaman yang relevan, dan independensi; dan
   b. 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 perundang-undangan;
   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 TIK. Asisten Auditor harus sudah mengikuti sosialisasi Audit TIK;
   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 Audit 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 Audit TIK, auditor harus:
   a) Mampu menjamin tujuan Audit TIK tercapai sesuai dengan ketentuan peraturan perundang-undangan;
   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 Kementerian.
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 basis 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;
      f) Batasan dan kendala yang ditemui selama proses Audit TIK;
      g) Tata cara pendistribusian laporan sesuai dengan surat penugasan.
   3. Laporan hasil 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.
   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;
   b) Audit Aplikasi Khusus SPBE;
   c) Audit Keamanan SPBE; dan
   d) Audit Pengelolaan TIK oleh Pihak Eksternal.
2. Cakupan Audit TIK dapat dilakukan secara terpisah sesuai kebutuhan.

b. Audit Infrastruktur SPBE

1. Melakukan Audit TIK Infrastruktur SPBE 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 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 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.
    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. 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 pascaimplementasi 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 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.

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Putranta Setyanugraha, SH. MSi.
NIP. 196212251993011001