PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

NOMOR TAHUN 2015

TENTANG

PEDOMAN TEKNIS AUDIT
MANAJEMEN KEAMANAN SISTEM ELEKTRONIK
PADA PENYELENGGARA PELAYANAN PUBLIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA,

Menimbang :

a. bahwa sesuai ketentuan dalam Pasal 14 huruf b Peraturan Menteri Komunikasi dan Informatika Nomor .... Tahun 2015 tentang Audit Penyelenggaraan Sistem Elektronik pada Penyelenggara Pelayanan Publik;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Menteri Komunikasi dan Informatika tentang Pedoman Teknis Audit Sistem Manajemen Keamanan Sistem Elektronik pada Penyelenggara Pelayanan Publik;

Mengingat :

1. 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);

2. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

3. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);

4. 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);

5. Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 127, Tambahan

Lembaran Negara Republik Indonesia Nomor 4890);

6. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 215, Tambahan Lembaran Negara Republik Indonesia Nomor 5357);

7. Peraturan Menteri Komunikasi dan Informatika Nomor 17/PER/M.KOMINFO/10/2010 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika;

8. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/KEM.KOMINFO/11/2007 Tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi;

10. Peraturan Menteri Komunikasi dan Informatika Nomor …….. Tentang Audit Penyelenggaraan Sistem Elektronik pada Penyelenggara Pelayanan Publik;

MEMUTUSKAN :

Menetapkan : PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA TENTANG PEDOMAN TEKNIS AUDIT MANAJEMEN KEAMANAN ELEKTRONIK PADA PENYELENGGARA PELAYANAN PUBLIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Penyelenggara Pelayanan Publik adalah setiap institusi penyelenggara negara, korporasi, lembaga independen yang dibentuk berdasarkan undang-undang untuk kegiatan pelayanan publik, dan badan hukum lain yang dibentuk semata-mata untuk kegiatan pelayanan publik;

2. Penyelenggaraan Sistem Elektronik adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, orang, badan usaha, dan/atau masyarakat.

3. Penyelenggara Sistem Elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik baik sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

4. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

5. Integritas Sistem Elektronik adalah suatu sistem yang memiliki kualitas informasi yang akurat, lengkap dan tidak rusak saat dipindahkan atau diperoses, serta dapat dicegah atau dihindari dari perbuatan yang tidak dikehendaki oleh pihak yang tidak berwenang

6. Audit Penyelenggaraan Sistem Elektronik adalah proses sistematis mengumpulkan dan mengevaluasi bukti untuk menentukan secara independen dan obyektif suatu sistem elektronik telah diselenggarakan secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya.

7. Audit Manajemen Keamanan Sistem Elektronik adalah proses sistematis mengumpulkan dan mengevaluasi bukti untuk menentukan secara independen dan obyektif suatu sistem elektronik telah menyusun, melaksanakan, mengevaluasi dan meningkatkan keamanan sistem elektronik dengan memadai.

Pasal 2

(1) Setiap penyelenggara sistem elektronik untuk pelayanan publik harus menyelenggarakan sistem elektronik secara aman.

(2) Untuk menjamin keamanan sistem elektronik untuk pelayanan publik sebagaimana dimaksud pada ayat (1) wajib dilakukan audit atas manajemen keamanan sistem elektronik.

BAB II
AUDIT MANAJEMEN KEAMANAN SISTEM ELEKTRONIK

Pasal 3

Metodologi audit manajemen keamanan sistem elektronik yang diatur dalam Peraturan Menteri ini meliputi:
a. tujuan;
b. cakupan;
c. tahapan;
d. pengujian.

Pasal 4

Tujuan audit manajemen keamanan sistem elektronik sebagaimana dimaksud dalam Pasal 3 huruf a adalah untuk mengevaluasi:
a. kerahasiaan sistem elektronik;
b. integritas sistem elektronik; dan
c. ketersediaan sistem elektronik;

Pasal 5

Cakupan audit manajemen keamanan sistem elektronik sebagaimana dimaksud dalam Pasal 3 huruf b sebagai berikut:
a. sistem manajemen keamanan sistem elektronik; dan

b. pengendalian keamanan sistem elektronik.

Pasal 6

Tahapan audit manajemen keamanan sistem elektronik sebagaimana dimaksud dalam Pasal 3 huruf c harus dilakukan sesuai ketentuan peraturan perundang-undangan.

Pasal 7

Audit sistem manajemen keamanan sistem elektronik dan pengendalian keamanan sistem elektronik sebagaimana dimaksud dalam Pasal 5 huruf a dan huruf b harus dilakukan sesuai dengan pedoman teknis sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB III
KETENTUAN PENUTUP

Pasal 8

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri Komunikasi dan Informatika ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal

MENTERI KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA,

RUDIANTARA

Diundangkan di Jakarta
pada tanggal

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

YASONNA H. LAOLY

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2015 NOMOR

LAMPIRAN
PERATURAN MENTERI KOMUNIKASIDAN INFORMATIKA REPUBLIK INDONESIA
NOMOR TAHUN 2015
TENTANG
PEDOMAN TEKNIS AUDIT MANAJEMEN KEAMANAN SISTEM ELEKTRONIK PENYELENGGARA PELAYANAN PUBLIK

PEDOMAN TEKNIS AUDIT MANAJEMEN KEAMANAN SISTEM ELEKTRONIK

A. AUDIT ATAS SISTEM MANAJEMEN KEAMANAN SISTEM ELEKTRONIK (SMKSE)

Pengujian dalam lingkup audit manajemen keamanan sistem elektronik pada cakupan Sistem Manajemen Keamanan sistem elektronik harus dilakukan pada setiap audit.

Dalam melaksanakan pengujian audit manajemen keamanan sistem elektronik auditor dapat menerapkan teknik audit masing-masing auditor, termasuk penggunaan teknik audit berbantuan komputer

1. Audit atas Penyusunan SMKSE

   a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi perencanaan SMKSE telah mencakup hal-hal sebagai berikut:

      1) Kebijakan tentang penyusunan, pelaksanaan, evaluasi dan peningkatan SMKSE;

      2) Bentuk komitmen manajemen terhadap pencapaian tujuan, penyediaan sumber daya SMKSE, dan peningkatan berkelanjutan SMKSE;

      3) Penetapan tujuan dan lingkup dari SMKSE, termasuk hal-hal yang dapat mempengaruhi pencapaian tujuan tersebut;

      4) Penetapan tujuan keamanan informasi pada setiap fungsi dan tingkatan yang relevan termasuk bagaimana cara mencapai tujuan tersebut.

      5) Identifikasi pihak-pihak yang terkait dengan SMKSE, termasuk kebutuhan dari masing-masing pihak;

      6) Penetapan peran, tanggung jawab, dan kewenangan dari pihak-pihak yang terkait dengan SMKSE;

      7) Identifikasi kebutuhan dan pemenuhan kompetensi yang diperlukan oleh setiap pihak yang terkait dengan SMKSE;

      8) Peningkatan kesadaran keamanan sistem elektronik setiap pihak yang terkait dengan SMKSE, termasuk kontribusi, manfaat, dan implikasi jika sesuai dengan SMKSE.

      9) Metode komunikasi internal dan eksternal yang diperlukan terkait dengan SMKSE;

      10) Pengendalian atas pembuatan, perubahan, dan penyimpanan dokumentasi informasi terkait SMKSE.

   b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi manajemen risiko keamanan sistem elektronik telah mencakup hal-hal sebagai berikut :

      1) Berbagai tindakan untuk menangani berbagai risiko dan kesempatan terkait keamanan sistem elektronik;

      2) Cara untuk mengintegrasikan dan mengimplementasikan berbagai tindakan tersebut ke dalam proses SMKSE;

      3) Cara mengevaluasi efektifitas dari berbagai tindakan tersebut.

c. Auditor harus melakukan evaluasi apakah rancangan dan implementasi proses penilaian risiko keamanan sistem elektronik telah mencakup hal-hal sebagai berikut:

1) Penetapan dan pemeliharaan kriteria keamanan risiko;

2) Penilaian risiko keamanan sistem elektronik yang hasilnya konsisten, valid dan dapat diperbandingkan;

3) Identifikasi berbagai risiko keamanan sistem elektronik;

4) Analisis berbagai risiko keamanan sistem elektronik;

5) Evaluasi berbagai risiko keamanan sistem elektronik.

d. Auditor harus melakukan evaluasi apakah rancangan dan implementasi proses penanganan risiko keamanan sistem elektronik telah mencakup hal-hal sebagai berikut :

1) Pemilihan opsi penangan risiko risiko keamanan sistem elektronik yang layak sesuai dengan hasil penilaian risiko keamanan sistem elektronik;

2) Penentuan pengendalian yang dibutuhkan untuk melaksanakan opsi penanganan risiko keamanan sistem elektronik yang telah dipilih;

3) Penyusunan rencana penanganan risiko keamanan sistem elektronik;

4) Persetujuan dari pemiik risiko atas rencana penanganan risiko keamanan sistem elektronik serta tingkat risiko residualnya.

2. Audit atas Pelaksanaan SMKSE

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian dukungan manajemen atas SMKSE telah mencakup hal-hal sebagai berikut :

1) Kebutuhan sumber daya dalam rangka perancangan dan implementasi SMKSE telah diidentifikasi dan disediakan dengan memadai;

2) Kebutuhan kompetensi untuk setiap personil yang melaksanakan pengendalian yang berpengaruh terhadap SMKE telah diidentifikasi, disediakan, dipelihara, dikembangkan, dievaluasi dan didokumentasikan dengan memadai;

3) Setiap personil yang menjadi bagian dari pengendalian SMKSE telah menyadari dan memahami kebijakan keamanan sistem elektronik, peranan masing-masing dalam sistem manajemen keamanan sistem elektronik termasuk manfaat peningkatan keamanan sistem elektronik serta dampak dari ketidaksesuaian dengan sistem manajemen keamanan sistem elektronik;

4) Ketentuan mengenai komunikasi dengan pihak internal dan pihak eksternal terkait sistem manajemen keamanan sistem elektronik telah ditetapkan dan dilaksanakan;

5) Ketentuan tentang berbagai dokumentasi informasi yang diharuskan oleh sistem manajemen keamanan sistem elektronik, mencakup pembuatan dan pemeliharaan serta pengendalian dokumentasi tersebut telah ditetapkan dan dilaksanakan.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian operasional SMKSE telah mencakup hal-hal sebagai berikut :

1) Organisasi telah menyusun, melaksanakan dan mengendalikan berbagai proses untuk dapat memenuhi persyaratan keamanan sistem elektronik, serta melaksanakan berbagai rencana tindakan yang telah ditetapkan;

2) Organisasi telah mengimplementasikan berbagai rencana untuk mencapai tujuan-tujuan keamanan sistem elektronik yang telah ditetapkan;

3) Organisasi telah mengelola dokumentasi informasi secara memadai untuk memperoleh keyakinan bahwa berbagai proses keamanan sistem elektronik telah dilaksanakan sesuai rencana;

4) Organisasi telah mengendalikan perubahan terencana dan melakukan reviu atas berbagai perubahan yang tidak terencana, serta mengambil tindakan untuk memitigasi dampak yang tidak diinginkan;

5) Organisasi harus memastikan bahwa berbagai proses yang dialihdayakan telah ditetapkan dan dikendalikan;

6) Organisasi telah melaksanakan analisis risiko keamanan sistem elektronik secara periodik atau pada saat terdapat perubahan yang signifikan, baik terencana atau tidak, dan dokumentasi hasil analisis risiko telah dipelihara dengan memadai.

3. Audit atas Evaluasi SMKSE

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pemantauan, pengukuran, analisis dan evaluasi SMKSE telah mencakup hal-hal sebagai berikut :

1) Organisasi telah melakukan evaluasi atasa kinerja keamanan sistem elektronik, dan efektifitas SMKSE;

2) Organisasi telah menetapkan hal-hal apa saja yang perlu dipantau dan diukur, termasuk proses dan pengendalian keamanan sistem elektronik;

3) Metode yang digunakan dalam melakukan pemantauan, pengukuran, analisis dan evaluasi dapat memberikan hasil yang valid;

4) Organisasi telah memelihara dokumentasi informasi yang memadai sebagai bukti hasil pelaksanaan pemantauan dan pengukuran;

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian audit intern SMKSE telah mencakup hal-hal sebagai berikut :

1) Organisasi telah melakukan audit intern pada periode yang telah direncanakan yang dapat memberikan informasi apakah SMKSE telah sesuai dengan persyaratan organisasi untuk SMKSE dan telah diimplementasikan dan dipelihara secara efektif;

2) Organisasi harus menyusun, menetapkan, menerapkan, dan memelihara berbagai kegiatan audit, termasuk frekuensi, metodologi, tanggungjawab, dan persyaratan perencanaan dan pelaporan, dimana kegiatan audit tersebut harus memperhatikan proses-proses yang menjadi perhatian dan hasil dari audit-audit sebelumnya;

3) Organisasi harus mendefinisikan kriteria dan lingkup untuk setiap audit;

4) Organisasi harus memilih audit dan melaksanakan audit yang dapat memastikaan obyektifitas dan imparsialitas dari proses audit;

5) Organisasi harus memastikan bahwa hasil audit dilaporkan kepada manajemen terkait;

6) Organisasi harus memelihara dokumentasi informasi sebagai bukti pelaksanaan dan hasil audit;

c. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian reviu manajemen atas SMKSE telah mencakup hal-hal sebagai berikut :

1) Pimpinan organisasi telah melakukan reviu atas SMKSE mereka sesuai periode yang telah direncanakan untuk memastikan kesesuaian, kelayakan, dan efektifitas SMKSE;

2) Reviu manajemen telah mempertimbangkan : status rencana tindak lanjut dari reviu sebelumnya; perubahan dalam berbagai masalah internal dan eksternal yang terkait dengan SMKSE; masukan dari kinerja keamanan sistem elektronik; masukan dari pihak-pihak yang terkait; hasil dari analisis risiko dan status rencana penanganan risiko; potensi-potensi peningkatan berkesinambungan;

3) Hasil dari reviu manajemen telah mencakup berbagai keputusan terkait potensi peningkatan berkesinambungan dan berbagai kebutuhan lainnya akan perubahan atas SMKSE.

4) Organisasi telah memelihara dokumentasi informasi sebagai bukti atas hasil reviu manajemen.

4. Audit atas Peningkatan SMKSE

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian peningkatan SMKSE telah mencakup hal-hal sebagai berikut :

1) Ketika ketidaksesuaian terjadi, organisasi harus bereaksi terhadap ketidaksesuaian, dan sesuai dengan keadaan dapat mengambil tindakan untuk mengendalikan dan memperbaikinya; atau menangani konsekuensi dari ketidaksesuaian tersebut;

2) Ketika ketidaksesuaian terjadi, organisasi harus mengevaluasi perlunya tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang atau terjadi di tempat lain;

3) Tindakan perbaikan telah sesuai dengan dampak dari ketidaksesuaian yang dihadapi;

4) Organisasi harus menyimpan informasi didokumentasikan sebagai bukti dari ketidaksesuaian dan tindaklanjutnya, dan hasil dari setiap tindakan korektif.

5) Organisasi harus terus meningkatkan kelayakan, kecukupan dan efektivitas sistem manajemen keamanan;

B. AUDIT ATAS PENGENDALIAN KEAMANAN SISTEM ELEKTRONIK

Pengujian dalam lingkup audit manajemen keamanan sistem elektronik pada cakupan Pengendalian Keamanan sistem elektronik dapat disesuaikan dengan kondisi masing-masing sistem elektronik.

Dalam melaksanakan pengujian audit manajemen keamanan sistem elektronik auditor dapat menerapkan teknik audit masing-masing auditor, termasuk penggunaan teknik audit berbantuan komputer.

1. Audit atas Kebijakan Keamanan

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Kebijakan Keamanan telah mencakup hal-hal sebagai berikut:

1) Berbagai kebijakan keamanan informasi telah ditetapkan dan disetujui oleh manajemen, dipublikasikan dan dikomunikasikan kepada karyawan dan pihak eksternal yang terkait;

2) Kebijakan keamanan informasi telah memperhatikan berbagi persyaratan yang berasal dari: strategi bisnis, peraturan, perundang-undangan dan kontrak, lingkungan ancaman keamanan informasi yang ada saat ini dan yang diproyeksi.

3) Kebijakan keamanan informasi telah berisi pernyataan mengenai: definisi keamanan informasi, tujuan dan prinsip-prinsip untuk memandu seluruh kegiatan yang berkaitan dengan keamanan informasi, pembagian tanggung jawab umum dan khusus untuk manajemen keamanan informasi kepada berbagai peranan yang telah didefinisikan; proses untuk penanganan penyimpangan dan pengecualian.

4) Pada tingkatan yang lebih rendah, kebijakan keamanan informasi telah dilengkapi dengan berbagai kebijakan khusus, yang menjabarkan lebih lanjut implementasi pengendalian keamanan informasi dimana biasanya disusun sesuai dengan kebutuhan kelompok sasaran tertentu di dalam suatu organisasi atau untuk mengatur topik-topik tertentu.

5) Kebijakan-kebijakan ini telah dikomunikasikan kepada karyawan dan pihak eksternal yang terkait, dalam bentuk yang sesuai, mudah diakses, dan dapat dipahami oleh audien yang dituju.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Reviu atas Kebijakan Keamanan telah mencakup hal-hal sebagai berikut :

1) Berbagai kebijakan keamanan informasi telah direviu sesuai periode yang direncanakan atau jika terjadi perubahan yang signifikan, untuk memastikan kesesuaian, kecukupan dan efektivitas kebijakan tersebut.

2) Setiap kebijakan harus memiliki pemilik yang telah menyetujui tanggung jawab manajemen untuk pengembangan, reviu dan evaluasi kebijakan tersebut. Reviu tersebut harus mencakup identifikasi peluang perbaikan atas kebijakan dan pendekatan organisasi dalam mengelola keamanan informasi untuk merespon perubahan lingkungan organisasi, keadaan bisnis, kondisi hukum atau lingkungan teknis.

3) Reviu kebijakan untuk keamanan informasi telah memperhatikan hasil reviu manajemen.

4) Telah terdapat persetujuan manajemen atas kebijakan yang direvisi.

2. Audit atas Organisasi Keamanan

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Organisasi Internal telah mencakup hal-hal sebagai berikut :

1) Seluruh tanggung jawab keamanan informasi telah didefinisikan dan dialokasikan;

2) Tugas dan bidang tanggung jawab yang dapat menimbulkan konflik telah dipisahkan untuk mengurangi peluang modifikasi yang tidak sah atau tidak disengaja atau penyalahgunaan aset organisasi;

3) Kontak yang sesuai dengan otoritas yang terkait telah dipelihara.

4) Kontak yang sesuai dengan kelompok kepentingan khusus atau forum spesialis keamanan dan asosiasi profesi lainnya telah dipelihara.

5) Keamanan informasi telah dipertimbangkan dalam manajemen proyek, terlepas dari jenis proyek.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Perangkat Bergerak dan *Teleworking* telah mencakup hal-hal sebagai berikut :

1) Kebijakan dan langkah-langkah keamanan yang mendukungnya telah diadopsi untuk mengelola risiko terkait dengan menggunakan perangkat bergerak.

2) Kebijakan dan langkah-langkah keamanan yang mendukungnya telah diterapkan untuk melindungi informasi yang diakses, diproses atau disimpan di lokasi *teleworking*.

3. Audit atas Keamanan Personil

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Sebelum Masa Kerja telah mencakup hal-hal sebagai berikut:

1) Penelitian verifikasi latar belakang pada semua calon tenaga kerja telah dilakukan sesuai dengan hukum, peraturan dan etika dan harus sebanding dengan kebutuhan bisnis, klasifikasi informasi yang dapat diakses dan persepsi risiko yang terkait.

2) Perjanjian kontrak dengan karyawan dan kontraktor telah menyatakan tanggung jawab mereka dan tanggung jawab organisasi untuk keamanan informasi.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Selama Masa Kerja telah mencakup hal-hal sebagai berikut :

1) Manajemen telah mewajibkan seluruh karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur organisasi yang ditetapkan

2) Semua karyawan dan kontraktor yang terkait telah memperoleh pendidikan dan pelatihan kesadaran keamanan yang sesuai, dan berbagai pembaharuan rutin atas kebijakan dan prosedur organisasi, yang relevan dengan fungsi pekerjaan mereka.

3) Telah terdapat proses pendisiplinan ynag formal dan dikomunikasikan untuk mengambil tindakan terhadap karyawan yang telah melakukan suatu pelanggaran keamanan informasi.

c. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Penghentian dan Perubahan Pekerjaan telah menetapkan tanggung jawab dan tugas keamanan informasi yang tetap berlaku setelah pemutusan atau perubahan pekerjaan, dikomunikasikan kepada karyawan atau kontraktor dan ditegakkan.

4. Audit atas Manajemen Asset

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Tanggung Jawab atas Aset telah mencakup hal-hal sebagai berikut:

1) Aset yang terkait dengan informasi dan fasilitas pengolahan informasi telah diidentifikasi, dan inventarisasi aset-aset ini telah disusun dan dipelihara.

2) Aturan untuk penggunaan yang dapat diterima dari informasi dan aset yang terkait dengan informasi dan fasilitas pengolahan informasi telah diidentifikasi, didokumentasikan dan diterapkan.

3) Semua karyawan dan pengguna pihak eksternal telah mengembalikan semua aset organisasi yang mereka miliki pada saat pemutusan hubungan kerja mereka, kontrak atau perjanjian

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Klasifikasi Informasi telah mencakup hal-hal sebagai berikut:

1) Informasi telah diklasifikasikan dalam hal persyaratan hukum, nilai, kritikalitas dan sensitifitas terhadap pengungkapan yang tidak sah atau modifikasi.

2) Prosedur pelabelan informasi yang layak telah dikembangkan dan dilaksanakan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.

3) Prosedur penanganan aset telah dikembangkan dan implementasi sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi

c. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Penanganan Media Data telah mencakup hal-hal sebagai berikut:

1) Prosedur telah diterapkan untuk pengelolaan *removablemedia* sesuai dengan skema klasifikasi yang diadopsi oleh organisasi.

2) Media telah dibuang dengan aman bila tidak lagi diperlukan, melalui prosedur yang resmi.

3) Media yang berisi informasi telah dilindungi dari akses ilegal, penyalahgunaan, dan kerusakan selama dipindahkan.

5. Audit atas Manajemen Akses

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Kebutuhan Bisnis atas Manajemen Akses telah mencakup hal-hal sebagai berikut :

1) Kebijakan pengendalian akses telah ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi.

2) Pengguna hanya disediakan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk mereka gunakan.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Manajemen Akses Pengguna telah mencakup hal-hal sebagai berikut :

1) Suatu proses formal pendaftaran dan penghapusan pengguna telah dilaksanakan dalam pemberian hak akses.

2) Suatu proses formal penyediaan akses pengguna telah diterapkan untuk memberikan atau mencabut hak akses untuk semua jenis pengguna untuk semua jenis sistem dan layanan.

3) Pemberian dan penggunaan hak akses istimewa telah dibatasi dan dikendalikan.

4) Pemberian informasi otentikasi rahasia telah dikendalikan melalui proses manajemen yang formal.

5) Pemilik aset telah meninjau hak akses pengguna secara berkala.

6) Hak akses dari seluruh karyawan dan pengguna pihak eksternal untuk informasi dan fasilitas pengolahan informasi telah dihapus setelah pemutusan hubungan kerja, kontrak atau perjanjianmereka, atau disesuaikan pada setiap perubahan.

c. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Tanggung Jawab Pengguna telah mengharuskan pengguna

untuk mengikuti praktek-praktek organisasi dalam penggunaan informasi otentikasi dengan rahasia.

d. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Pengendalian Akses atas Sistem dan Aplikasitelah mencakup hal-hal sebagai berikut:

1) Akses terhadap informasi dan berbagai fungsi sistem aplikasi telah dibatasi sesuai dengan kebijakan pengendalian akses.

2) Jika diharuskan oleh kebijakan pengendalian akses, akses ke sistem dan aplikasi telah dikendalikan dengan prosedur *log-on*yang aman.

3) Sistem manajemen kata sandi telahdilakukan dengan interaktif dan mampu memastikan kualitas kata sandi.

4) Penggunaan program utilitas yang mungkin mampu mengesampingkan pengendalian sistem dan aplikasi telah dibatasi dan dikendalkan dengan ketat.

5) Akses ke kode sumber program telah dibatasi.

6. Audit atas Kriptografi.

   Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Kriptografi telah mencakup hal-hal sebagai berikut :

   1) Kebijakan tentang penggunaan pengendalian kriptografi untuk perlindungan informasi telah disusun dan diimplementasikan.

   2) Kebijakan tentang penggunaan, perlindungan dan masa pakai kunci kriptografi telah disusun dan dilaksanakan pada seluruh siklus kunci kriptografi.

7. Audit atas Keamanan Fisik dan Lingkungan.

   a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Area Aman telah mencakup hal-hal sebagai berikut :

      1) Batasan keamanan telah didefinisikan dan digunakan untuk melindungi area-area kerja yang berisi informasi dan fasilitas pengolahan informasi baik yang sensitif maupun yang penting.

      2) Area aman telah dilindungi oleh pengendalian yang sesuai untuk memastikan bahwa hanya karyawan yang berhak saja yang diperbolehkan untuk memasuki.

      3) Keamanan fisik untuk kantor-kantor, berbagai ruangan dan fasilitas telah dirancang dan diterapkan.

      4) Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan telah dirancang dan diterapkan.

      5) Prosedur untuk bekerja di area aman telah dirancang dan diterapkan.

      6) Jalur akses seperti area pengiriman dan titik bongkar muat di mana orang yang tidak berwenang bisa memasuki lokasi telah dikendalikan dan, jika dimungkinkan, terisolasi dari fasilitas pengolahan informasi untuk menghindari akses yang tidak sah.

   b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Peralatan telah mencakup hal-hal sebagai berikut :

1) Peralatan telah diletakkan dan dilindungi untuk mengurangi risiko dari ancaman dan bahayalingkungan, dan potensiadanya akses yang tidak sah.

2) Peralatan telah dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dari utilitas pendukung.

3) Kabel listrik dan telekomunikasi yang membawa data atau mendukung layanan informasi telah dilindungi dari intersepsi, gangguan atau kerusakan.

4) Peralatan telah dipelihara dengan benar untuk memastikan keberlanjutan ketersediaan dan integritasnya.

5) Peralatan, informasi atau perangkat lunak tidak diambil dari lokasi tanpa izin sebelumnya.

6) Keamanan telah diterapkan untuk berbagi aset diluar kantor dengan mempertimbangkan berbagai risiko dari kegiatan bekerja di luar kantor.

7) Setiap satuan peralatan yang mengandung media penyimpanan telah diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa dengan aman sebelum dibuang atau digunakan kembali.

8) Pengguna telah memastikan bahwa peralatan yang sedangtanpa pengawasan memiliki perlindungan yang tepat.

9) Kebijakan meja bersih dari kertas dan media penyimpanan sementara dan kebijakan layar bersih untuk fasilitas pengolahan informasi telah diadopsi.

8. Audit atas Keamanan Operasional

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Prosedur dan Tanggung Jawab Operasional telah mencakup hal-hal sebagai berikut :

1) Berbagai prosedur operasional telah didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya.

2) Perubahan pada organisasi, proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi telah dikendalikan.

3) Penggunaan sumber daya telah dimonitor, disesuaikan dan kebutuhan kapasitas di masa depan telah diperkirakan untuk memastikan kinerja sistem yang diperlukan.

4) Pengembangan, pengujian, dan lingkungan operasional telahdipisahkan untuk mengurangi risiko akses yang tidak sah atau perubahan atas lingkungan operasional.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Perlindungan dari *Malware* telah mencakup deteksi, pencegahan dan pemulihan pengendalian untuk melindungi terhadap malware dilaksanakan, dikombinasikan dengan kesadaran pengguna yang sesuai.

c. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian *Backup* telah mencakup salinan cadangan informasi, perangkat lunak dan sistem gambar harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan disepakati.

d. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian *Logging* dan *Monitoring* telah mencakup hal-hal sebagai berikut:

   1) Berbagai log kejadian merekam kegiatan pengguna, eksepsi, kesalahan dan kejadian keamanan informasi telah dibuat, disimpan dan direviu secara berkala.

   2) Fasilitas *logging* dan informasi log telah dilindungi terhadap gangguan dan akses yang tidak sah.

   3) Kegiatan administrator dan operator sistem telah dicatat dan log dilindungi dan direviu secara berkala.

   4) Jam dari semua sistem pengolahan informasi yang relevan dalam suatu organisasi atau domain keamanan telah disinkronisasikan ke referensi sumber waktu tunggal.

e. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian atas Perangkat Lunak Operasional telah mencakup prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional.

f. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Manajemen Kerentanan Teknis telah mencakup hal-hal sebagai berikut:

   1) Informasi tentang kerentanan teknis dari sistem informasi yang digunakan telah diperoleh secara tepat waktu, paparan organisasi terhadap kerentanan tersebut telah dievaluasi dan tindakan yang tepat telah diambil untuk mengatasi risiko yang terkait.

   2) Aturan yang mengatur instalasi perangkat lunak oleh pengguna telah ditetapkan dan dilaksanakan.

g. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Pertimbangan Audit Sistem Informasi telah mencakup persyaratan audit dan kegiatan yang melibatkan verifikasi sistem operasional telah direncanakan dengan hati-hati dan disepakati untuk meminimalkan gangguan terhadap proses bisnis.

9. Audit atas Keamanan Komunikasi.

   a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Manajemen Keamanan Jaringan telah mencakup hal-hal sebagai berikut :

1) Jaringan telah dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi.

2) Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan telah diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan, baik layanan ini disediakan secara mandiri ataupun alih daya.

3) Kelompok-kelompok layanan informasi, pengguna dan sistem informasi telah dipisahkan di dalam jaringan.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Manajemen Pengiriman Informasi telah mencakup hal-hal sebagai berikut :

1) Kebijakan, prosedur dan pengendalian formal atas pengiriman informasi telah tersedia untuk melindungi pengiriman informasi melalui penggunaan semua jenis fasilitas komunikasi.

2) Berbagai perjanjian yang ada telah membahas pengiriman informasi bisnis secara aman antara organisasi dan pihak eksternal.

3) Informasi yang terkait dalam pesan elektronik telah dilindungi dengan layak.

4) Persyaratan untuk perjanjian kerahasiaan atau tiada-pengungkapan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi telah diidentifikasi, berkala dan didokumentasikan.

10. Audit atas Keamanan Akuisi, Pengembangan, dan Pemeliharaan Sistem.

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Ketentuan Keamanan Sistem Informasi telah mencakup hal-hal sebagai berikut:

1) Persyaratan yang terkait keamanan informasi telah dimasukkan dalam persyaratan untuk sistem informasi baru atau tambahan untuk sistem informasi yang ada.

2) Informasi yang terlibat dalam layanan aplikasi yang melalui jaringan publik telah dilindungi dari aktivitas penipuan, perselisihan perjanjian dan pengungkapan yang tidak sah dan modifikasi.

3) Informasi yang terlibat dalam transaksi layanan aplikasi telah dilindungi untuk mencegah pengiriman yang tidak lengkap, kesalahan pengiriman, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi atau pengulangan pesan yang tidak sah.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Keamanan dalam Proses Pengembangan dan Dukungan telah mencakup hal-hal sebagai berikut:

1) Aturan untuk pengembangan perangkat lunak dan sistem telah ditetapkan dan diterapkan untuk seluruh pengembangan di dalam organisasi.

2) Perubahan sistem yang dalam siklus pengembangan telah dikendalikan dengan menggunakan prosedur pengendalian perubahan yang formal.

3) Ketika sistem operasi berubah, aplikasi bisnis penting telah ditinjau dan diuji untuk memastikan tidak ada dampak negatif terhadap operasi atau keamanan organisasi.

4) Modifikasi atas perangkat lunak paket harus dihindari, terbatas pada perubahan yang diperlukan dan semua perubahan telah dikendalikan secara ketat.

5) Prinsip untuk rekayasa sistem keamanantelah ditetapkan, didokumentasikan, dipelihara dan diterapkan untuk setiap upaya implementasi sistem informasi.

6) Organisasi telah menetapkan dan melindungi dengan baik lingkungan pengembangan yang aman untuk berbagai upaya pengembangan sistem dan integrasi yang mencakup seluruh siklus hidup pengembangan sistem.

7) Organisasi telah mengawasi dan memantau kegiatan pengembangan sistem yang dialihdayakan.

8) Pengujian fungsionalitas keamanan telah dilakukan selama pengembangan.

9) Program pengujian dan kriteria terkait penerimaan telah ditetapkan untuk sistem informasi baru, peningkatan dan versi baru.

c. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Data Pengujian telah mencakup data uji telah dipilih dengan hati-hati, dilindungi dan dikendalikan.

11. Audit atas Keamanan Hubungan dengan Rekanan.

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Keamanan Informasi dalam Hubungan dengan Rekanan telah mencakup hal-hal sebagai berikut :

1) Persyaratan keamanan informasi untuk mengurangi risiko yang terkait dengan akses rekanan atas aset organisasi telah disepakati dengan rekanan dan didokumentasikan.

2) Semua persyaratan keamanan informasi yang relevan telahditetapkan dan disetujui oleh setiap rekanan yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastrukturTI untuk informasi organisasi.

3) Perjanjian dengan rekanan telah mencakup persyaratan untuk mengatasi risiko keamanan informasi yang terkait dengan teknologi informasi dan komunikasi dalam rantai pasokan produkdan layanan.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Manajemen Pelaksanaan Layanan Rekanan telah mencakup hal-hal sebagai berikut :

1) Organisasi telah secara teratur memonitor, mereviu dan mengaudit pelaksanaan layanan dari rekanan.

2) Perubahan pada penyediaan jasa oleh rekanan, termasuk menjaga dan meningkatkan keamanan informasi kebijakan, prosedur dan pengendalian yang sudah ada, telah dikelola, dengan memperhatikan kekritisan informasi bisnis, sistem dan proses yang terlibat dan penilaian kembali risiko.

12. Audit atas Manajemen Insiden Keamanan Informasi.

    Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Manajemen Insiden dan Peningkatan Keamanan Informasitelah mencakup hal-hal sebagai berikut :

    1) Tanggung jawab dan prosedur manajemen telah ditetapkan untuk memastikan respon yang cepat, efektif dan teratur terhadap insiden keamanan informasi.
    2) Kejadian keamanan informasi telah dilaporkan melalui saluran manajemen yang tepat secepat mungkin.
    3) Karyawan dan kontraktor menggunakan sistem dan layanan informasi organisasi telah diwajibkanuntuk mencatat dan melaporkan setiap kelemahan keamanan informasi yang diamati atau dicurigai dalam sistem atau layanan.
    4) Kejadian keamanan informasi telah dinilai dan diputuskan jika mereka harus diklasifikasikan sebagai insiden keamanan informasi.
    5) Insiden keamanan informasi telah ditindaklanjuti sesuai dengan prosedur yang terdokumentasi.
    6) Pengetahuan yang diperoleh dari analisis dan menyelesaikan insiden keamanan informasi telah digunakan untuk mengurangi kemungkinan atau dampak dari insiden di masa depan
    7) Organisasi telah menetapkan dan menerapkan prosedur untuk identifikasi, pengumpulan, akuisisi dan pelestarian informasi, yang dapat berfungsi sebagai bukti.

13. Audit atas Aspek Keamanan Informasi dalam Manajemen Kontinuitas Bisnis.

    a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Kontinuitas Keamanan Informasitelah mencakup hal-hal sebagai berikut:

        1) Organisasi telah menetapkan persyaratan untuk keamanan informasi dan kelangsungan manajemen keamanan informasi dalam situasi yang merugikan, misalnya selama krisis atau bencana.
        2) Organisasi telah menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan pengendalian untuk memastikan tingkat kontinuitas yang diperlukan untuk keamanan informasi selama situasi yang merugikan.
        3) Organisasi telah memverifikasi secara berkala pengendalian kontinuitas keamanan yang telah ditetapkan dan dilaksanakan untuk memastikan bahwa mereka adalah tepat dan efektif dalam situasi yang merugikan.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Redudansi telah mencakup keharusan fasilitas pengolahan informasi telah diimplementasikan dengan redundansi yang cukup untuk memenuhi kebutuhan ketersediaan.

14. Audit atas Kepatuhan

a. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Kepatuhan kepada Persyaratan Perundangan dan Kontraktual telah mencakup hal-hal sebagai berikut:

1) Semua undang-undang legislatif yang relevan, peraturan, persyaratan kontrak dan pendekatan organisasi untuk memenuhi persyaratan ini telahsecara eksplisit diidentifikasi, didokumentasikan dan terus diperbaharui untuk setiap sistem informasi dan organisasi.

2) Prosedur yang tepat telah diterapkan untuk memastikan kepatuhan dengan persyaratan legislatif, peraturan dan kontrak yang terkait dengan hak kekayaan intelektual dan penggunaan produk perangkat lunak berpemilik.

3) Rekaman telah dilindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah dan tidak sah rilis, sesuai dengan perundangan, peraturan, kontrak dan persyaratan bisnis.

4) Privasi dan perlindungan informasi pribadi telah dijamin sebagaimana dipersyaratkan dalam undang-undang dan peraturan yang berlaku di mana yang relevan.

5) Pengendalian kriptografi telah digunakan sesuai dengan semua perjanjian yang relevan, undang-undang dan peraturan.

b. Auditor harus melakukan evaluasi apakah rancangan dan implementasi pengendalian Reviu Keamanan Informasi telah mencakup hal-hal sebagai berikut :

1) Pendekatan organisasi untuk mengelola keamanan informasi dan pelaksanaannya (tujuan pengendalian, pengendalian, kebijakan, proses dan prosedur untuk keamanan informasi) telah dikaji secara independen pada interval yang direncanakan atau ketika perubahan signifikan terjadi.

2) Manajemen telah secara teratur meninjau kepatuhan pengolahan informasi dan prosedur dalam bidang tanggung jawab mereka dengan kebijakan dan standar keamanan yang sesuai dan persyaratan keamanan lainnya.

3) Sistem informasi telah ditinjau secara rutin untuk mematuhi kebijakan dan standar keamanan informasi organisasi.

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA,

RUDIANTARA