INTERNATIONAL STANDARD

ISO/IEC 27005

Information technology – Security techniques – Information security risk management

Reference number
ISO/IEC 27005:2008(E)

Daftar Isi

Daftar Gambar

Daftar Tabel

Prakata

ISO (*the International Organization for Standardization*) dan IEC (*the International Electrotechnical Commission*) membentuk sistem khusus untuk standardisasi di seluruh dunia. Badan nasional yang menjadi anggota ISO atau IEC berpartisipasi dalam pengembangan Standar Internasional melalui komite teknis yang ditetapkan oleh organisasi masing-masing untuk menangani bidang-bidang khusus kegiatan teknis. ISO dan IEC komite teknis berkolaborasi dalam bidang kepentingan bersama. Organisasi internasional lainnya, pemerintah dan non-pemerintah, bersama ISO dan IEC, juga ambil bagian dalam pekerjaan. Dalam bidang teknologi informasi, ISO dan IEC telah membentuk komite teknis bersama, ISO/IEC JTC 1.

Standar Internasional dikonsepkan menurut aturan yang diberikan dalam ISO/IEC *Directives*, *Part* 2.

Tugas utama dari komite teknis bersama adalah untuk mempersiapkan Standar Internasional. Konsep International Standar yang diadopsi oleh komite teknis bersama diedarkan ke badan nasional untuk pemungutan suara. Penerbitan sebagai Standar Internasional menghendaki persetujuan oleh sekurang-kurangnya 75% dari badan nasional yang memberikan suara.

Perlu diperhatikan kemungkinan bahwa beberapa elemen dari dokumen ini mungkin menjadi subyek dari hak paten. ISO dan IEC tidak bertanggung jawab untuk mengidentifikasi hak setiap atau semua paten tersebut.

ISO/IEC 27005 dipersiapkan oleh *Joint Technical Committee* ISO/IEC JTC 1, Teknologi Informasi, Subkomite SC 27, Teknik Keamanan TI.

Edisi pertama ISO/IEC 27005 ini membatalkan dan menggantikan ISO/IEC TR 13335-3:1998, dan ISO/IEC TR 13335-4:2000, yang merupakan revisi teknis.

Pendahuluan

Standar ini memberikan pedoman untuk Manajemen Risiko Keamanan Informasi dalam suatu organisasi, mendukung khususnya persyaratan Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan ISO/IEC 27001. Namun, standar ini tidak menyediakan metodologi khusus untuk manajemen risiko keamanan informasi. Terserah organisasi untuk menentukan pendekatan mereka dengan manajemen risiko, tergantung misalnya pada ruang lingkup SMKI, konteks manajemen risiko, atau sektor industri. Sejumlah metodologi yang ada dapat digunakan dalam kerangka dijelaskan dalam standar ini untuk menerapkan persyaratan SMKI.

Standar ini relevan dengan manajer dan staf yang bersangkutan dengan risiko keamanan informasi manajemen dalam suatu organisasi dan, di mana, pihak eksternal yang sesuai mendukung kegiatan tersebut.

Teknologi informasi – Teknik keamanan – Manajemen risiko keamanan informasi

1. Ruang Lingkup

Standar ini memberikan pedoman manajemen risiko keamanan informasi.

Standar ini mendukung konsep umum yang ditetapkan dalam ISO/IEC 27001 dan dirancang untuk membantu pelaksanaan yang memuaskan dari keamanan informasi berdasarkan pendekatan manajemen risiko.

Pengetahuan tentang konsep, model, proses dan terminologi yang dijelaskan dalam ISO/IEC 27001 dan ISO/IEC 27002 penting bagi pemahaman yang lengkap dari Standar Internasional ini.

Standar ini berlaku pada semua jenis organisasi (misalnya perusahaan komersial, instansi pemerintah, organisasi non-profit) yang berniat untuk mengelola risiko yang dapat membahayakan keamanan informasi organisasi.

2. Acuan normatif

Dokumen acuan berikut sangat diperlukan untuk penerapan dokumen ini. Untuk acuan bertanggal, hanya edisi yang dikutip berlaku. Untuk acuan tidak bertanggal, edisi terakhir dokumen acuan (termasuk setiap amandemen) yang berlaku.
ISO/IEC 27001:2005, teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi – Persyaratan.
ISO/IEC 27002:2005, teknologi informasi - Teknik keamanan - Kode praktek untuk manajemen keamanan informasi.

3. Istilah dan definisi

Untuk tujuan dokumen ini, istilah dan definisi yang diberikan dalam ISO/IEC 27001 dan ISO/IEC 27002 berikut berlaku:

3.1
dampak
perubahan yang merugikan pada tingkat tujuan bisnis tercapai

3.2
risiko keamanan informasi
potensi bahwa ancaman yang diberikan akan mengeksploitasi kerentanan aset atau kelompok aset dan dengan demikian menyebabkan kerugian kepada organisasi

CATATAN Hal ini diukur dalam hal kombinasi kemungkinan dari suatu peristiwa dan konsekuensinya.

3.3
penghindaran risiko
keputusan untuk tidak terlibat, atau tindakan menarik diri dari situasi risiko

[ISO/IEC *Guide* 73:2002]

3.4
komunikasi risiko
pertukaran atau berbagi informasi mengenai risiko antara pembuat keputusan dan pemangku kepentingan yang lain

[ISO/IEC *Guide* 73:2002]

3.5
perkiraan risiko
proses untuk memberikan nilai pada probabilitas dan konsekuensi dari suatu risiko

[ISO/IEC *Guide* 73:2002]

CATATAN 1 dalam konteks standar ini, istilah "kegiatan" digunakan sebagai pengganti istilah "proses" untuk perkiraan risiko

CATATAN 2 dalam konteks standar ini, istilah "kemungkinan" digunakan sebagai pengganti istilah "probabilitas" untuk perkiraan risiko

3.6
identifikasi risiko
proses untuk menemukan, menginventaris, dan menggolongkan unsur risiko

[ISO/IEC *Guide* 73:2002]

CATATAN dalam konteks standar ini, istilah "kegiatan" digunakan sebagai pengganti istilah "proses" untuk identifikasi risiko

3.7
pengurangan risiko
tindakan yang diambil untuk mengurangi probabilitas, dampak negatif, atau keduanya, dikaitkan dengan suatu risiko

[ISO/IEC *Guide* 73:2002]

CATATAN dalam konteks standar ini, istilah "kemungkinan" digunakan sebagai pengganti istilah "probabilitas" untuk pengurangan risiko

3.8
retensi risiko
penerimaan beban kerugian atau manfaat keuntungan dari suatu risiko tertentu

[ISO/IEC *Guide* 73:2002]

CATATAN dalam konteks risiko keamanan informasi, hanya dampak negatif (kerugian) yang dianggap sebagai retensi risiko

3.9
pemindahan risiko
berbagi beban kerugian atau manfaat keuntungan untuk suatu risiko

[ISO/IEC *Guide* 73:2002]

CATATAN dalam konteks risiko keamanan informasi, hanya dampak negatif (kerugian) yang dianggap sebagai pemindahan risiko

4. Struktur standar internasional ini

Standar ini memuat gambaran proses manajemen risiko keamanan informasi dan kegiatan-kegiatannya.

Informasi latar belakang disediakan dalam klausul 5.

Gambaran umum dari proses manajemen risiko keamanan informasi disediakan dalam klausul 6.

Semua kegiatan manajemen risiko keamanan informasi seperti yang disajikan dalam Klausul 6 yang kemudian dijelaskan dalam klausul-klausul berikut:

- Penetapan konteks dalam Klausul 7,
- Penilaian risiko dalam Klausul 8,
- Perlakuan resiko dalam Klausul 9,
- Penerimaan Risiko dalam Klausul 10,
- Komunikasi risiko dalam Klausul 11,
- Pemantauan dan peninjauan risiko dalam Klausul 12.

Informasi tambahan untuk kegiatan manajemen risiko keamanan informasi disajikan dalam lampiran-lampiran. Penetapan konteks didukung oleh Lampiran A (mendefinisikan ruang lingkup dan batasan dari proses manajemen risiko keamanan informasi). Identifikasi dan penilaian aset serta penilaian dampak dibahas dalam Lampiran B (contoh untuk aset), Lampiran C (contoh ancaman khas), dan Lampiran D (contoh kerentanan khas).

Contoh-contoh pendekatan manajemen risiko keamanan informasi disajikan dalam Lampiran E.

Batasan untuk pengurangan risiko disajikan dalam Lampiran F.

Seluruh kegiatan manajemen risiko yang disajikan dari Klausul 7 sampai dengan Klausul 12 disusun sebagai berikut:

Masukan : mengidentifikasi informasi apapun yang dibutuhkan untuk melakukan suatu kegiatan.

Tindakan : menjelaskan kegiatan.

Pedoman pelaksanaan : memberikan pedoman untuk melakukan tindakan. Beberapa pedoman ini mungkin tidak cocok dalam semua kasus dan cara-cara lain sehingga melakukan tindakan yang mungkin lebih tepat.

Keluaran : mengidentifikasi setiap informasi yang diperoleh setelah melakukan kegiatan.

5. Latar Belakang

Suatu pendekatan sistematis terhadap manajemen risiko keamanan informasi diperlukan untuk mengidentifikasi kebutuhan organisasi mengenai persyaratan keamanan informasi dan menciptakan sistem manajemen keamanan informasi yang

efektif (SMKI). Pendekatan ini harus sesuai untuk lingkungan organisasi, dan khususnya harus diselaraskan dengan manajemen risiko perusahaan secara keseluruhan. Upaya keamanan harus menangani risiko secara efektif dan tepat waktu di mana dan kapan mereka dibutuhkan. SMKI harus menjadi bagian integral dari semua kegiatan manajemen keamanan informasi dan harus diterapkan baik untuk pelaksanaan dan operasi yang sedang berlangsung dari SMKI.

Informasi manajemen risiko keamanan harus menjadi proses yang berkelanjutan. Proses ini harus menetapkan konteks, menilai resiko dan penanganan resiko menggunakan rencana perlakuan untuk melaksanakan rekomendasi dan keputusan. Manajemen risiko menganalisa apa yang bisa terjadi dan apa konsekuensi yang mungkin bisa, sebelum memutuskan apa yang harus dilakukan dan kapan, untuk mengurangi risiko ke tingkat yang dapat diterima.

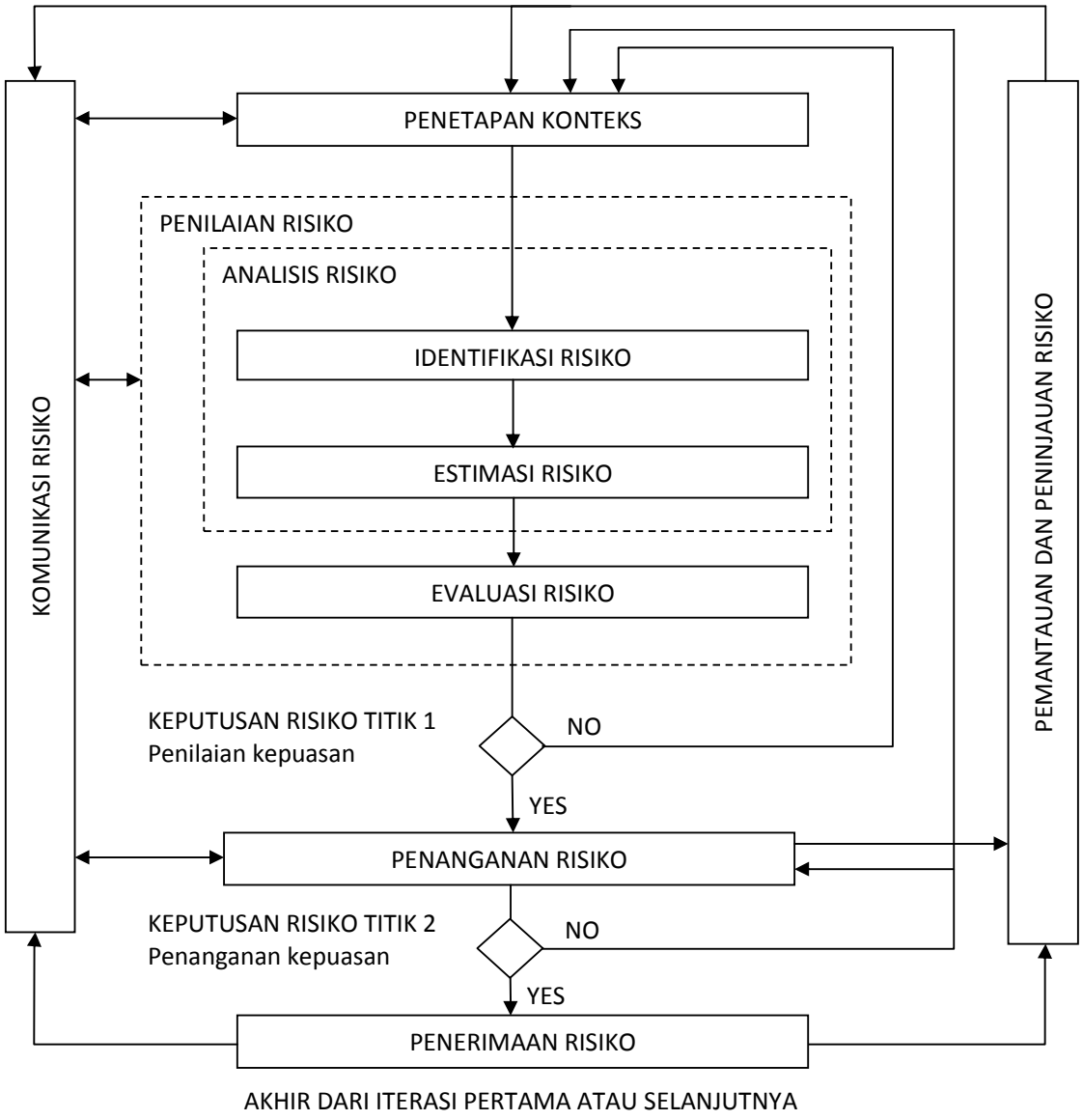
Informasi manajemen risiko keamanan harus berkontribusi pada hal-hal berikut:

1 Risiko yang diidentifikasi;
2 Risiko yang dinilai dalam hal konsekuensi mereka untuk bisnis dan kemungkinan terjadinya;
3 Kemungkinan dan konsekuensi risiko ini sedang dikomunikasikan dan dipahami;
4 Urutan prioritas untuk perlakuan resiko yang didirikan;
5 Prioritas tindakan untuk mengurangi risiko yang terjadi;
6 Para pemangku kepentingan terlibat ketika keputusan manajemen risiko dibuat dan selalu diinformasikan mengenai status manajemen risiko;
7 Efektivitas pemantauan perlakuan risiko;
8 Risiko dan proses manajemen risiko dipantau dan dikaji secara berkala;
9 Informasi ditangkap untuk meningkatkan pendekatan manajemen risiko;
10 Manajer dan staf dididik tentang risiko dan tindakan yang diambil untuk menanggulanginya.

Proses manajemen risiko keamanan informasi dapat diterapkan pada organisasi secara keseluruhan, setiap bagian diskrit organisasi (misalnya departemen, lokasi fisik, layanan), setiap sistem informasi, aspek yang ada atau yang direncanakan atau kontrol tertentu (misalnya perencanaan kelangsungan bisnis).

6. Gambaran tentang proses manajemen risiko keamanan informasi

Proses manajemen risiko keamanan informasi terdiri dari penetapan konteks (Klausul 7), penilaian risiko (Klausul 8), perlakuan risiko (Klausul 9), penerimaan risiko (Klausul 10), komunikasi risiko (Klausul 11), serta pemantauan dan pengkajian risiko (Klausul 12).



Gambar 1 - Proses manajemen risiko keamanan informasi

Seperti yang digambarkan pada Gambar 1, proses manajemen risiko keamanan informasi dapat berulang untuk penilaian risiko dan/atau kegiatan perlakuan risiko. Pendekatan iteratif untuk melakukan penilaian risiko dapat meningkatkan kedalaman dan rincian dari penilaian pada setiap iterasi. Pendekatan berulang itu memberikan keseimbangan yang baik antara meminimalkan waktu dan usaha yang dihabiskan dalam mengidentifikasi kontrol, sementara masih memastikan bahwa risiko tinggi dinilai dengan tepat.

Konteksnya ditetapkan terlebih dahulu. Kemudian penilaian risiko dilakukan. Jika hal ini memberikan informasi yang cukup untuk secara efektif menentukan tindakan yang diperlukan untuk memodifikasi risiko ke tingkat yang dapat diterima, maka tugas selesai dan selanjutnya menentukan perlakuan risiko. Jika informasi tidak cukup, iterasi lain dari

penilaian risiko dengan konteks revisi (misalnya kriteria evaluasi risiko, kriteria penerimaan risiko atau kriteria dampak) akan dilakukan, mungkin pada bagian terbatas dari seluruh ruang lingkup (lihat Gambar 1, Keputusan Risiko Titik 1) .

Keefektifan perlakuan risiko tergantung pada hasil penilaian risiko. Ada kemungkinan bahwa perlakuan risiko tidak akan langsung mengarah pada tingkat risiko residual yang dapat diterima. Dalam situasi ini, iterasi lain dari penilaian risiko dengan konteks parameter yang berubah (misalnya kriteria penilaian, penerimaan risiko atau dampak risiko), jika perlu, mungkin diperlukan, diikuti dengan perlakuan risiko lebih lanjut (lihat Gambar 1, Keputusan Risiko Titik 2).

Kegiatan penerimaan risiko harus memastikan risiko residual secara eksplisit diterima oleh para pengelola organisasi. Hal ini penting terutama dalam situasi di mana pelaksanaan kontrol diabaikan atau ditunda, misalnya karena biaya.

Selama proses manajemen risiko keamanan informasi adalah penting bahwa risiko dan penanganannya dikomunikasikan kepada manajer dan staf operasional yang tepat. Bahkan sebelum penanganan risiko, informasi tentang risiko yang teridentifikasi dapat sangat berharga untuk mengelola insiden dan dapat membantu untuk mengurangi potensi kerusakan. Kesadaran oleh para manajer dan staf risiko, jenis kontrol yang ada untuk mengurangi risiko dan bidang yang menjadi perhatian organisasi membantu dalam berurusan dengan insiden dan kejadian tak terduga dengan cara yang paling efektif. Hasil rinci dari setiap kegiatan proses manajemen risiko keamanan informasi dan dari dua poin keputusan risiko harus didokumentasikan.

ISO/IEC 27001 menetapkan bahwa pengendalian yang diterapkan dalam ruang lingkup, batasan-batasan dan konteks SMKI harus berbasis risiko. Penerapan proses manajemen risiko keamanan informasi dapat memenuhi persyaratan ini. Ada banyak pendekatan dimana proses dapat berhasil dilaksanakan dalam suatu organisasi. Organisasi harus menggunakan apa pun pendekatan yang paling sesuai keadaan mereka untuk setiap aplikasi yang spesifik dari proses.

Dalam SMKI, menetapkan konteks, penilaian risiko, mengembangkan rencana penanganan dan penerimaan risiko adalah bagian dari fase "rencana". Dalam fase "melakukan" dari SMKI, tindakan dan kontrol yang diperlukan untuk mengurangi risiko ke tingkat yang dapat diterima dilaksanakan sesuai dengan rencana penanganan. Dalam fase "pemeriksaan" dari SMKI, manajer akan menentukan kebutuhan untuk perbaikan penilaian risiko dan perlakuan risiko mengingat insiden dan perubahan keadaan. Dalam fase "tindakan", setiap tindakan yang diperlukan, termasuk aplikasi tambahan dari proses manajemen risiko keamanan informasi, dilakukan.

Tabel berikut merangkum kegiatan manajemen risiko keamanan informasi yang relevan dengan empat tahapan proses SMKI:

Tabel 1 - Penyelarasan antara SMKI dan Proses Manajemen Risiko Keamanan

Proses SMKI	Proses Manajemen Risiko Keamanan Informasi
Perencanaan	Menetapkan konteks Penilaian risiko Mengembangkan rencana penanganan risiko Penerimaan risiko
Melakukan	Penerapan rencanan penanganan risiko
Pemeriksaan	Pemantauan dan peninjauan berkala terhadap risiko
Tindakan	Meningkatkan dan memelihara Proses Manajemen Risiko Keamanan Informasi

7. Penetapan konteks

7.1. Pertimbangan umum

Masukan: Semua informasi tentang organisasi yang relevan dengan penetapan konteks manajemen risiko keamanan informasi.

Tindakan: konteks manajemen risiko keamanan informasi harus ditetapkan, yang melibatkan penetapan kriteria dasar yang diperlukan untuk manajemen risiko keamanan informasi (7.2), mendefinisikan ruang ruang lingkup dan batasan-batasan (7.3), dan membentuk sebuah organisasi yang layak menjalankan manajemen risiko keamanan informasi (7,4).

Pedoman pelaksanaan:
Hal ini penting untuk menentukan tujuan dari manajemen risiko keamanan informasi karena ini akan mempengaruhi keseluruhan proses dan pembentukan konteks tertentu, tujuan ini dapat berupa:

1. mendukung SMKI
2. kepatuhan hukum dan bukti *due diligence* (uji tuntas)
3. penyusunan rencana kelangsungan bisnis
4. persiapan rencana respon insiden
5. deskripsi tentang persyaratan keamanan informasi untuk suatu produk, layanan atau mekanisme

Pedoman pelaksanaan untuk elemen penetapan konteks diperlukan untuk mendukung SMKI selanjutnya akan dibahas dalam Klausul 7.2, 7.3 dan 7.4 di bawah ini.

CATATAN ISO/IEC 27001 tidak menggunakan istilah "konteks". Namun, semua Klausul 7 terkait dengan persyaratan "menentukan ruang lingkup dan batasan SMKI" [4.2.1 a)], "mendefinisikan kebijakan SMKI" [4.2.1 b)] dan "menentukan pendekatan penilaian risiko" [4.2 .1 c)], ditetapkan dalam ISO/IEC 27001.

Hasil : Spesifikasi kriteria dasar, ruang lingkup dan batas-batas, dan organisasi untuk proses manajemen risiko keamanan informasi.

7.2. Kriteria dasar

Tergantung pada ruang lingkup dan tujuan dari manajemen risiko, pendekatan yang berbeda dapat diterapkan. Pendekatan ini juga mungkin berbeda untuk setiap iterasi.

Sebuah pendekatan manajemen risiko yang tepat harus dipilih atau dikembangkan yang membahas kriteria dasar seperti: kriteria evaluasi risiko, kriteria dampak, kriteria penerimaan risiko.

Selain itu, organisasi harus menilai apakah sumber daya yang diperlukan tersedia untuk:

- Melakukan penilaian risiko dan menetapkan rencana penanganan;
- Mendefinisikan dan menerapkan kebijakan dan prosedur, termasuk pelaksanaan kontrol yang dipilih;
- Memantau control;
- Memantau proses manajemen risiko keamanan informasi.

CATATAN Lihat juga ISO/IEC 27001 (Klausul 5.2.1) mengenai penyediaan sumber daya untuk penerapan dan operasional SMKI.

Kriteria evaluasi risiko
kriteria evaluasi risiko harus dikembangkan untuk mengevaluasi risiko keamanan informasi organisasi dengan mempertimbangkan hal-hal berikut:

- Nilai strategis dari proses informasi bisnis
- Tingkat kritikalitas aset informasi yang terlibat
- Persyarayan hukum dan peraturan, serta kewajiban kontraktual
- Ketersediaan, kerahasiaan dan integritas dari operasional dan bisnis yang penting
- Harapan dan persepsi pemangku kepentingan, dan konsekuensi negatif untuk perbuatan baik dan reputasi

Selain itu, kriteria evaluasi risiko dapat digunakan untuk menentukan prioritas pada perlakuan risiko.

Kriteria dampak
Kriteria Dampak harus dikembangkan dan ditetapkan dalam hal tingkat kerusakan atau kerugian organisasi yang disebabkan oleh kejadian keamanan informasi mempertimbangkan hal-hal berikut:

- Tingkat klasifikasi aset informasi yang terkena dampak
- Pelanggaran keamanan informasi (misalnya hilangnya kerahasiaan, integritas dan ketersediaan)
- Gangguan operasi (pihak internal atau ketiga)
- Kerugian bisnis dan nilai keuangan
- Gangguan rencana dan tenggat waktu
- Kerusakan reputasi
- Pelanggaran terhadap persyaratan hukum, peraturan atau kontrak

CATATAN Lihat juga ISO/IEC 27001 [Klausul 4.2.1 d) 4] mengenai identifikasi kriteria dampak terhadap kerugian kerahasiaan, integritas dan ketersediaan.

Kriteria penerimaan risiko

Kriteria penerimaan risiko harus dikembangkan dan ditetapkan. Kriteria penerimaan risiko sering bergantung pada kebijakan, tujuan, sasaran organisasi serta kepentingan dari pemangku kepentingan.

Sebuah organisasi harus menetapkan sendiri skala untuk tingkat penerimaan risiko. Berikut hal-hal harus dipertimbangkan selama pengembangan:

- kriteria penerimaan risiko dapat mencakup beberapa ambang batas, dengan target level risiko yang diinginkan, tetapi ketetapan manajer senior untuk menerima risiko diatas level ini dalam keadaan yang telah didefinisikan.
- kriteria penerimaan risiko dapat dinyatakan sebagai rasio keuntungan yang telah diperkirakan (atau manfaat bisnis lainnya) terhadap risiko estimasi.
- kriteria penerimaan risiko yang berbeda mungkin berlaku untuk kelas risiko yang berbeda, misalnya risiko yang dapat mengakibatkan ketidakpatuhan terhadap peraturan atau hukum tidak dapat diterima, sedangkan penerimaan risiko tinggi dapat diizinkan jika ini ditentukan sebagai persyaratan kontrak.
- kriteria penerimaan risiko dapat mencakup persyaratan untuk penanganan tambahan di masa depan, misalnya risiko dapat diterima jika ada persetujuan dan komitmen untuk mengambil tindakan mengurangi risiko ke level yang dapat diterima dalam jangka waktu yang ditetapkan.

Kriteria penerimaan risiko mungkin berbeda sesuai dengan berapa lama risiko diharapkan ada, misalnya risiko mungkin terkait dengan kegiatan sementara atau jangka pendek. Kriteria penerimaan risiko harus dibentuk mengingat hal-hal berikut:

- Kriteria Bisnis
- Aspek hukum dan peraturan
- Operasi
- Teknologi
- Keuangan
- Faktor sosial dan kemanusiaan

CATATAN Kriteria penerimaan risiko sesuai dengan "kriteria untuk menerima risiko dan mengidentifikasi level risiko yang dapat diterima" ditentukan dalam ISO/IEC 27001 Klausul 4.2.1 c) 2).

Informasi lebih lanjut dapat ditemukan di Lampiran A.

7.3. Ruang lingkup dan batasan

Organisasi harus menentukan ruang lingkup dan batas-batas manajemen risiko keamanan informasi.

Ruang lingkup dari proses manajemen risiko keamanan informasi perlu ditetapkan untuk memastikan bahwa semua aset yang relevan diperhitungkan dalam penilaian risiko. Selain itu, batas-batas perlu diidentifikasi [lihat juga ISO/IEC 27001 Klausul 4.2.1 a)] untuk mengatasi risiko-risiko yang mungkin timbul melalui batas-batas tersebut.

Informasi tentang organisasi harus dikumpulkan untuk menentukan lingkungan dimana organisasi tersebut berberoperasi dan relevansinya dengan proses manajemen risiko keamanan informasi.

Ketika mendefinisikan ruang lingkup dan batas-batas, organisasi harus mempertimbangkan informasi berikut:

- Tujuan, strategi, dan kebijakan bisnis strategis organisasi;
- Proses bisnis;
- Fungsi dan struktur organisasi;
- Persyaratan hukum, peraturan dan kontrak yang berlaku untuk organisasi;
- Kebijakan keamanan informasi organisasi tersebut;
- Pendekatan keseluruhan organisasi untuk manajemen risiko;
- Aset Informasi;
- Lokasi organisasi dan karakteristik geografisnya;
- Kendala yang mempengaruhi organisasi;
- Ekspektasi pemangku kepentingan;
- Lingkungan sosial budaya;
- Antarmuka (misalnya pertukaran informasi dengan lingkungan).

Selain itu, organisasi harus memberikan justifikasi untuk setiap pengecualian dari ruang lingkup.

Contoh lingkup manajemen risiko antara lain aplikasi TI, infrastruktur TI, proses bisnis, atau bagian dari sebuah organisasi yang telah didefinisikan.

CATATAN Ruang lingkup dan batas-batas dari manajemen risiko keamanan informasi berkaitan dengan ruang lingkup dan batas-batas SMKI yang diperlukan dalam ISO/IEC 27001 4.2.1 a).

Informasi lebih lanjut dapat ditemukan di Lampiran A.

7.4. Organisasi manajemen risiko keamanan informasi

Organisasi dan tanggung jawab untuk proses manajemen risiko keamanan informasi harus dibentuk dan dipelihara. Berikut ini adalah peran dan tanggung jawab utama organisasi ini:

- Pengembangan proses manajemen risiko keamanan informasi yang sesuai bagi organisasi;
- Identifikasi dan analisis pemangku kepentingan;
- Definisi peran dan tanggung jawab semua pihak baik internal maupun eksternal organisasi;

- Penetapan hubungan yang diperlukan antara organisasi dan pemangku kepentingan, serta antarmuka untuk fungsi manajemen risiko tingkat tinggi organisasi (misalnya manajemen risiko operasional), serta antarmuka untuk proyek-proyek atau kegiatan lain yang relevan;
- Definisi jalur eskalasi keputusan;
- Spesifikasi catatan untuk disimpan;

Organisasi ini harus disetujui oleh manajer-manajer organisasi yang tepat.

CATATAN ISO/IEC 27001 membutuhkan kebulatan tekad dan penyediaan sumber daya yang dibutuhkan untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara dan meningkatkan SMKI [5.2.1 a)]. Organisasi untuk operasi manajemen risiko dapat dianggap sebagai salah satu sumber daya yang diperlukan oleh ISO/IEC 27001.

8. Penilaian risiko keamanan informasi

8.1. Gambaran umum dari penilaian risiko keamanan informasi

CATATAN Kegiatan penilaian risiko disebut sebagai proses dalam ISO/IEC 27001.

Masukan : Kriteria dasar, ruang lingkup dan batas-batas, dan organisasi untuk proses manajemen risiko keamanan informasi yang didirikan.

Tindakan : Risiko harus diidentifikasi, diukur atau digambarkan secara kualitatif, dan diprioritaskan terhadap kriteria evaluasi risiko dan tujuan yang relevan dengan organisasi.

Pedoman pelaksanaan:
Risiko adalah kombinasi dari dampak yang akan mengikuti dari terjadinya suatu peristiwa yang tidak diinginkan dan kemungkinan terjadinya peristiwa tersebut. Penilaian risiko mengukur atau menggambarkan secara kualitatif suatu risiko dan memungkinkan manajer untuk memprioritaskan risiko sesuai dengan keseriusan yang mereka rasakan atau kriteria lain yang telah ditetapkan.

Penilaian risiko memuat kegiatan-kegiatan berikut:

- Analisa risiko (Klausul 8.2) yang terdiri dari:
  - Identifikasi risiko (Klausul 8.2.1);
  - Estimasi risiko (Klausul 8.2.2),
- Evaluasi risiko (Klausul 8.3).

Penilaian risiko menentukan nilai aset informasi, mengidentifikasi ancaman-ancaman yang berlaku dan kerentanan yang ada (atau bisa ada), mengidentifikasi kontrol yang ada dan efeknya pada risiko yang teridentifikasi, menentukan konsekuensi potensial dan akhirnya memprioritaskan risiko yang diperoleh dan menggolongkan mereka terhadap kriteria evaluasi risiko yang diatur dalam penetapan konteks.

Penilaian risiko sering dilakukan dalam dua (atau lebih) iterasi. Pertama, penilaian tingkat tinggi dilakukan untuk mengidentifikasi risiko yang berpotensi tinggi yang memerlukan penilaian lebih lanjut. Iterasi berikutnya dapat melibatkan pertimbangan mendalam lebih lanjut terhadap risiko berpotensi tinggi yang

diungkapkan dalam iterasi awal. Dimana hal ini memberikan informasi yang tidak cukup untuk menilai risiko maka analisis rinci lebih lanjut dilakukan, mungkin pada bagian-bagian dari seluruh ruang lingkup, dan mungkin menggunakan metode yang berbeda.

Terserah kepada organisasi untuk memilih pendekatan sendiri untuk penilaian risiko berdasarkan sasaran dan tujuan dari penilaian risiko.

Pembahasan pendekatan penilaian risiko keamanan informasi dapat ditemukan dalam Lampiran E.

Hasil: Sebuah daftar risiko yang telah dinilai dan diprioritaskan menurut risiko kriteria evaluasi.

8.2. Analisis risiko

8.2.1. Identifikasi risiko

8.2.1.1. Pengenalan terhadap identifikasi risiko

Tujuan dari identifikasi risiko adalah untuk menentukan apa yang bisa terjadi untuk menyebabkan potensi kerugian, dan untuk mendapatkan wawasan tentang bagaimana, di mana dan mengapa kerugian yang mungkin terjadi. Langkah-langkah yang dijelaskan dalam subklausul 8.2.1 berikut harus mengumpulkan data masukan untuk kegiatan estimasi risiko.

CATATAN Kegiatan dijelaskan dalam klausul berikutnya dapat dilakukan dalam urutan yang berbeda tergantung pada metodologi yang digunakan.

8.2.1.2. Identifikasi aset-aset

Masukan: Cakupan dan batas-batas untuk penilaian risiko yang akan dilakukan, daftar konstituen dengan pemilik, lokasi, fungsi, dll

Tindakan : Aset dalam ruang lingkup ditetapkan harus diidentifikasi (berhubungan dengan ISO/IEC 27001, Klausul 4.2.1 d) 1)).

Pedoman pelaksanaan:
Aset adalah sesuatu yang bernilai bagi organisasi dan yang karenanya membutuhkan perlindungan. Untuk identifikasi aset itu harus diingat bahwa sistem informasi terdiri dari lebih dari *hardware* dan *software*.

Identifikasi aset harus dilakukan pada level rincian yang sesuai sehingga memberikan cukup informasi untuk penilaian risiko. Level rincian yang digunakan pada identifikasi aset akan mempengaruhi jumlah keseluruhan informasi yang dikumpulkan selama penilaian risiko. Level tersebut dapat disempurnakan dalam iterasi lebih lanjut dari penilaian risiko.

Seorang pemilik aset harus diidentifikasi untuk setiap aset, untuk memberikan tanggung jawab dan akuntabilitas untuk aset tersebut.

Pemilik aset mungkin tidak memiliki hak milik atas aset, tetapi memiliki tanggung jawab untuk pembuatan, pengembangan, pemeliharaan, penggunaan dan keamanan yang sesuai. Pemilik aset seringkali adalah orang yang paling cocok untuk menentukan nilai aset terhadap organisasi (lihat 8.2.2.2 untuk penilaian aset).

Tinjauan batas adalah perimeter aset dari organisasi ditetapkan untuk dikelola oleh proses manajemen risiko keamanan informasi.

Informasi lebih lanjut tentang identifikasi dan penilaian aset yang terkait dengan keamanan informasi dapat ditemukan dalam Lampiran B.

Hasil : Daftar aset menjadi risiko dikelola, dan daftar proses bisnis yang terkait dengan aset dan relevansinya.

8.2.1.3. Identifikasi ancaman

Masukan : Informasi tentang ancaman yang diperoleh dari meninjau insiden, pemilik aset, pengguna dan sumber-sumber lain, termasuk katalog ancaman eksternal.

Tindakan : Ancaman dan sumbernya harus diidentifikasi (berhubungan dengan ISO/IEC 27001, Klausul 4.2.1 d) 2)).

Pedoman pelaksanaan:
Ancaman memiliki potensi untuk membahayakan aset seperti informasi, proses dan sistem dan oleh karena itu organisasi. Ancaman mungkin berasal dari alam atau manusia, dan bisa tidak disengaja atau disengaja. Sumber ancaman baik tidak disengaja dan disengaja harus diidentifikasi. Ancaman mungkin timbul dari dalam atau dari luar organisasi. Ancaman harus diidentifikasi secara umum dan menurut jenis (misalnya tindakan yang tidak sah, kerusakan fisik, kegagalan teknis) dan kemudian di mana ancaman individu yang sesuai dalam kelas generik diidentifikasi.

Ini berarti tidak ada ancaman yang terlupakan, termasuk tak terduga, tetapi volume pekerjaan yang diperlukan terbatas.

Beberapa ancaman dapat mempengaruhi lebih dari satu aset. Dalam kasus seperti itu mereka dapat menyebabkan dampak yang berbeda tergantung pada aset yang terpengaruh.

Masukan untuk identifikasi ancaman dan perkiraan kemungkinan kejadian (lihat 8.2.2.3) dapat diperoleh dari pemilik aset atau pengguna, dari staf sumber daya manusia, dari manajemen fasilitas dan spesialis keamanan informasi, ahli keamanan fisik, departemen hukum dan organisasi lainnya termasuk badan hukum, otoritas cuaca, perusahaan

asuransi dan pemerintah nasional. Aspek lingkungan dan budaya harus dipertimbangkan ketika menangani ancaman.

Pengalaman internal dari insiden dan penilaian ancaman masa lalu harus dipertimbangkan dalam penilaian saat ini. Mungkin ada baiknya untuk memeriksa katalog ancaman lainnya (mungkin spesifik untuk sebuah organisasi atau bisnis) untuk melengkapi daftar ancaman umum, di mana relevan. Katalog ancaman dan statistik tersedia dari badan-badan industri, pemerintah nasional, badan hukum, perusahaan asuransi, dll.

Bila menggunakan katalog ancaman, atau hasil penilaian ancaman sebelumnya, maka harus disadari bahwa ada perubahan terus-menerus dari ancaman yang relevan, terutama jika lingkungan bisnis atau sistem informasi berubah.

Informasi lebih lanjut tentang jenis ancaman dapat ditemukan dalam Lampiran C.

Hasil : Sebuah daftar ancaman dengan identifikasi jenis ancaman dan sumbernya.

8.2.1.4. Identifikasi kontrol yang ada

Masukan : Dokumentasi kontrol, rencana implementasi perlakuan resiko.

Tindakan : Kontrol yang ada dan direncanakan harus diidentifikasi.

Pedoman pelaksanaan :
Identifikasi kontrol yang ada harus dilakukan untuk menghindari pekerjaan atau biaya yang tidak perlu, misalnya dalam duplikasi kontrol. Selain itu, sementara mengidentifikasi kontrol yang ada, pemeriksaan harus dilakukan untuk memastikan bahwa kontrol bekerja dengan benar - referensi untuk laporan audit SMKI yang ada harus membatasi waktu yang dihabiskan dalam tugas ini. Jika kontrol tidak bekerja seperti yang diharapkan, hal ini dapat menyebabkan kerentanan. Pertimbangan harus diberikan pada situasi di mana kontrol yang dipilih (atau strategi) gagal dalam operasi dan karenanya kontrol pelengkap yang diperlukan untuk mengatasi risiko yang diidentifikasi secara efektif. Dalam SMKI, menurut ISO/IEC 27001, hal ini didukung oleh pengukuran efektivitas pengendalian. Sebuah cara untuk memperkirakan dampak dari kontrol adalah untuk melihat bagaimana kontrol mengurangi kemungkinan ancaman dan kemudahan mengeksploitasi kerentanan, atau dampak dari kejadian tersebut.

Tinjauan manajemen dan laporan audit juga memberikan informasi tentang efektivitas kontrol yang ada.

Kontrol yang direncanakan akan dilaksanakan sesuai dengan rencana pelaksanaan perlakuan risiko harus dipertimbangkan dengan cara yang sama seperti yang sudah dilaksanakan.

Kontrol ada atau yang direncanakan dapat diidentifikasi sebagai tidak efektif, atau tidak cukup, atau tidak dibenarkan. Jika tidak dibenarkan atau tidak cukup, kontrol harus diperiksa untuk menentukan apakah kontrol itu harus dihapus, diganti dengan yang lain, kontrol yang lebih cocok, atau apakah harus tinggal di tempat, misalnya, karena alasan biaya.

Untuk identifikasi kontrol yang ada atau yang direncanakan, kegiatan berikut dapat membantu:

1. Meninjau dokumen yang berisi informasi tentang kontrol (misalnya, rencana pelaksanaan perlakuan risiko). Jika proses manajemen keamanan informasi didokumentasikan dengan baik semua kontrol yang ada atau yang direncanakan dan status pelaksanaannya harus tersedia;
2. Memeriksa dengan orang-orang yang bertanggung jawab untuk keamanan informasi (misalnya petugas keamanan informasi dan petugas keamanan sistem informasi, manajer pembangunan atau manajer operasi) dan pengguna sebagaimana kontrol benar-benar dilaksanakan untuk proses informasi atau sistem informasi yang dipertimbangkan;
3. Melakukan peninjauan *on-site* dari kontrol fisik, membandingkan yang diimplementasikan dengan daftar kontrol apa yang harus ada, dan memeriksa yang diterapkan, apakah mereka bekerja dengan benar dan efektif; atau
4. Meninjau hasil audit internal.

Hasil : Daftar semua kontrol yang ada dan direncanakan, implementasi dan status penggunaannya.

8.2.1.5. Identifikasi kerentanan

Masukan : Sebuah daftar ancaman yang diketahui, daftar aset dan kontrol yang ada.

Tindakan : Kerentanan yang dapat dieksploitasi oleh ancaman untuk membahayakan aset atau organisasi harus diidentifikasi (berhubungan dengan ISO/IEC 27001, Klausul 4.2.1 d) 3)).

Pedoman pelaksanaan :
Kerentanan dapat diidentifikasi dalam bidang-bidang berikut:

- Organisasi
- Proses dan prosedur
- Rutinitas manajemen
- Personel
- Lingkungan fisik

- Konfigurasi sistem Informasi
- Perangkat keras, perangkat lunak atau peralatan komunikasi
- Ketergantungan pada pihak luar

Keberadaan dari suatu kerentanan tidak menyebabkan bahaya, karena perlu ada ancaman yang hadir untuk memanfaatkannya.

Sebuah kerentanan yang tidak memiliki ancaman terkait mungkin tidak memerlukan pelaksanaan kontrol, tetapi harus dikenali dan dipantau untuk perubahan. Perlu dicatat bahwa penerapanyang tidak tepat atau tidak berfungsinya pengendalian atau pengendalian yang digunakan secara tidak benar bisa menjadi kerentanan. Kontrol dapat efektif atau tidak efektif tergantung pada lingkungan di mana ia beroperasi. Sebaliknya, ancaman yang tidak memiliki kerentanan yang sesuai mungkin tidak menimbulkan risiko.

Kerentanan dapat dikaitkan dengan sifat aset yang dapat digunakan dengan cara, atau untuk tujuan, selain yang dimaksudkan ketika aset dibeli atau dibuat. Kerentanan yang timbul dari sumber yang berbeda perlu dipertimbangkan, misalnya, kerentanan yang intrinsik atau ekstrinsik pada aset.

Contoh kerentanan dan metode untuk penilaian kerentanan dapat ditemukan di Lampiran D.

Hasil : Daftar kerentanan dalam kaitannya dengan aset, ancaman dan kontrol; daftar kerentanan yang tidak berhubungan dengan ancaman diidentifikasi untuk ulasan.

8.2.1.6. Identifikasi konsekuensi

Masukan : Daftar aset, daftar proses bisnis, dan daftar ancaman dan kerentanan, dimana tepat, terkait dengan aset dan relevansinya.

Tindakan : Konsekuensi bahwa kerugian atas kerahasiaan, integritas dan ketersediaan terhadap aset harus diidentifikasi (lihat ISO/IEC 27001 4.2.1 d) 4)).

Pedoman pelaksanaan :
Konsekuensi bisa jadi kehilangan efektivitas, kondisi operasi yang merugikan, kerugian bisnis, reputasi, kerusakan, dll.

Kegiatan ini mengidentifikasi kerusakan atau konsekuensi kepada organisasi yang dapat disebabkan oleh skenario insiden. Sebuah skenario insiden adalah deskripsi ancaman yang mengeksploitasi kerentanan tertentu atau serangkaian kerentanan dalam insiden keamanan informasi (lihat ISO/IEC 27002, Klausul 13). Dampak dari skenario Insiden akan ditentukan mempertimbangkan kriteria dampak yang telah didefinisikan selama kegiatan penetapan konteks. Hal ini dapat mempengaruhi satu atau lebih aset atau bagian dari aset.

Dengan demikian aset mungkin telah menetapkan nilai-nilai baik untuk biaya keuangan mereka dan karena konsekuensi bisnis jika mereka rusak atau dikompromikan.

Konsekuensi mungkin bersifat sementara atau mungkin permanen seperti dalam kasus perusakan aset.

CATATAN ISO/IEC 27001 menjelaskan terjadinya skenario insiden sebagai "kegagalan keamanan".

Organisasi harus mengidentifikasi konsekuensi operasional dari skenario insiden dalam hal (namun tidak terbatas pada):

1. Investigasi dan waktu perbaikan.
2. Waktu (kerja) yang hilang.
3. Peluang yang hilang.
4. Kesehatan dan keselamatan.
5. Biaya keuangan akan keterampilan khusus untuk memperbaiki kerusakan.
6. Kesan nama baik dan iktikad baik.

Rincian tentang penilaian kerentanan teknis dapat ditemukan dalam B.3. Penilaian Dampak.

Hasil : Daftar skenario insiden dengan konsekuensinya terkait dengan aset dan proses bisnis.

8.2.2. Estimasi risiko

8.2.2.1. Metodologi estimasi risiko

Analisis risiko dapat dilakukan dalam berbagai tingkat detail tergantung pada kritikalitas aset, jangkauan kerentanan yang diketahui, dan keterlibatan insiden sebelumnya dalam organisasi. Metodologi estimasi bisa kualitatif atau kuantitatif, atau kombinasi dari keduanya, tergantung pada keadaan. Dalam prakteknya, estimasi kualitatif sering digunakan mulanya untuk mendapatkan indikasi umum level risiko dan untuk mengungkapkan risiko utama.

Kemudian mungkin perlu untuk melakukan analisis yang lebih spesifik atau analisis kuantitatif pada risiko besar karena biasanya kurang kompleks dan lebih murah untuk melakukan analisis kualitatif daripada analisis kuantitatif.

Bentuk analisis harus konsisten dengan kriteria evaluasi risiko yang dikembangkan sebagai bagian dari penetapan konteks.

Rincian lebih lanjut dari metodologi estimasi akan dijelaskan:

(a) Estimasi kualitatif:
Estimasi kualitatif menggunakan skala kualifikasi atribut untuk menggambarkan besarnya konsekuensi potensial (misalnya Low,

Medium dan High) dan kemungkinan konsekuensi tersebut terjadi. Sebuah keuntungan dari estimasi kualitatif adalah kemudahan pemahamannya oleh semua personel yang relevan, sementara kerugian adalah ketergantungan pada pilihan subjektif dari skala.

Skala ini dapat diadaptasi atau disesuaikan agar sesuai dengan keadaan dan deskripsi yang berbeda dapat digunakan untuk risiko yang berbeda. Estimasi kualitatif dapat digunakan:

1. Sebagai kegiatan penyaringan awal untuk mengidentifikasi risiko yang memerlukan analisis yang lebih rinci;
2. Dimana analisis semacam ini cocok untuk keputusan;
3. Dimana data numerik atau sumber daya tidak memadai untuk estimasi kuantitatif

Analisis kualitatif harus menggunakan informasi faktual dan data yang tersedia.

(b) estimasi kuantitatif:
Estimasi kuantitatif menggunakan skala dengan nilai numerik (daripada skala deskriptif yang digunakan dalam estimasi kualitatif) untuk konsekuensi dan kemungkinan, menggunakan data dari berbagai sumber. Kualitas analisis tergantung pada keakuratan dan kelengkapan dari nilai-nilai numerik dan validitas dari model yang digunakan. Perkiraan kuantitatif dalam banyak kasus menggunakan data historis insiden, memberikan keuntungan yang dapat berhubungan langsung dengan tujuan keamanan informasi dan perhatian organisasi. Kerugiannya adalah kurangnya data tersebut pada risiko baru atau kelemahan keamanan informasi. Kelemahan dari pendekatan kuantitatif dapat terjadi dimana faktual, data yang diaudit tidak tersedia sehingga menciptakan ilusi nilai dan akurasi penilaian risiko.

Cara di mana konsekuensi dan kemungkinan disajikan dan cara-cara di mana mereka dikombinasikan untuk memberikan level risiko akan bervariasi sesuai dengan jenis risiko dan tujuan hasil penilaian risiko yang akan digunakan. Ketidakpastian dan variabilitas dari konsekuensi dan kemungkinan harus dipertimbangkan dalam analisis dan dikomunikasikan secara efektif.

8.2.2.2. Penilaian konsekuensi

Masukan : Daftar skenario insiden relevan yang diidentifikasi, termasuk identifikasi ancaman, kerentanan, aset yang terkena dampak, konsekuensi terhadap aset dan proses bisnis.

Tindakan : Dampak bisnis pada organisasi yang mungkin timbul dari informasi insiden keamanan yang mungkin atau aktual harus dinilai, dengan mempertimbangkan konsekuensi dari pelanggaran keamanan informasi seperti hilangnya kerahasiaan, integritas atau ketersediaan aset (berhubungan dengan ISO/IEC 27001, Klausul 4.2.1 e) 1)).

Pedoman pelaksanaan :
Setelah mengidentifikasi semua aset dalam tinjauan, nilai-nilai yang diberikan untuk aset-aset ini harus dipertimbangkan saat menilai konsekuensi.

Nilai dampak bisnis dapat dinyatakan dalam bentuk kualitatif dan kuantitatif, tetapi metode untuk menetapkan nilai moneter pada umumnya dapat memberikan informasi lebih untuk pengambilan keputusan dan karenanya memfasilitasi proses pembuatan keputusan lebih efisien.

Penilaian aset dimulai dengan klasifikasi aset sesuai dengan kritikalitas mereka, dalam hal kepentingan aset untuk memenuhi tujuan bisnis dari organisasi. Penilaian ini kemudian ditentukan dengan menggunakan dua ukuran:

1. nilai penggantian aset : biaya pembersihan pemulihan dan mengganti informasi (jika mungkin); dan
2. konsekuensi bisnis atas kehilangan atau kompromi aset, seperti potensi bisnis yang merugikan dan/atau konsekuensi hukum atau peraturan dari pengungkapan, modifikasi, tidak tersedia dan/atau perusakan informasi, dan aset-aset Informasi lain.

Penilaian ini dapat ditentukan dari analisis dampak bisnis. Nilai, ditentukan oleh konsekuensi terhadap bisnis, biasanya secara signifikan lebih tinggi daripada biaya penggantian sederhana, tergantung pada pentingnya aset bagi organisasi dalam mencapai tujuan bisnis.

Penilaian aset merupakan faktor kunci dalam penilaian dampak skenario insiden, karena kejadian tersebut dapat mempengaruhi lebih dari satu aset (misalnya aset yang saling tergantung), atau hanya bagian dari aset. Ancaman dan kerentanan yang berbeda akan memiliki dampak yang berbeda pada aset, seperti hilangnya kerahasiaan, Integritas atau ketersediaan.

Penilaian konsekuensi demikian terkait dengan penilaian aset berdasarkan pada analisis dampak bisnis.

Konsekuensi atau dampak bisnis dapat ditentukan dengan pemodelan hasil dari suatu peristiwa atau serangkaian peristiwa, atau dengan ekstrapolasi dari studi eksperimental atau data masa lalu.

Konsekuensi dapat dinyatakan dalam istilah kriteria dampak moneter, teknis atau manusia, atau kriteria lain yang relevan bagi organisasi. Dalam beberapa kasus, lebih dari satu nilai numerik diperlukan untuk menentukan konsekuensi untuk waktu, tempat, kelompok atau situasi yang berbeda.

Konsekuensi dalam waktu dan keuangan harus diukur dengan pendekatan yang sama digunakan untuk ancaman kemungkinan dan

kerentanan. Konsistensi harus dipertahankan pada pendekatan kuantitatif atau kualitatif.

Informasi lebih lanjut baik pada penilaian aset dan penilaian dampak dapat ditemukan dalam Lampiran B.

Hasil : Daftar konsekuensi yang dinilai dari skenario Insiden dinyatakan dengan mematuhi kriteria aset dan dampak.

8.2.2.3. Penilaian kemungkinan insiden

Masukan : Daftar skenario insiden relevan yang telah diidentifikasi, termasuk identifikasi ancaman, aset yang terkena dampak, kerentanan yang dieksploitasi dan konsekuensi terhadap aset dan proses bisnis. Selanjutnya, daftar semua kontrol yang ada dan direncanakan, efektivitas mereka, implementasi dan status penggunaan.

Tindakan : Kemungkinan skenario kejadian harus dinilai (berkaitan dengan ISO/IEC 27001, Klausul 4.2.1 e) 2)).

Pedoman pelaksanaan :
Setelah mengidentifikasi skenario insiden, perlu untuk menilai kemungkinan setiap skenario dan dampak yang terjadi, dengan menggunakan teknik estimasi kualitatif atau kuantitatif. Hal ini harus mempertimbangkan seberapa sering ancaman terjadi dan bagaimana mudahnya kerentanan dapat dieksploitasi, dengan mempertimbangkan:

- pengalaman dan statistik berlaku untuk kemungkinan ancaman .
- untuk sumber ancaman disengaja : motivasi dan kemampuan, yang akan berubah dari waktu ke waktu, dan sumber daya yang tersedia untuk memungkinkan penyerang, serta persepsi daya tarik dan kerentanan aset untuk kemungkinan penyerangan.
- untuk sumber ancaman disengaja : faktor geografis misalnya kedekatan dengan bahan kimia atau tanaman minyak bumi, kemungkinan kondisi cuaca ekstrim, dan faktor-faktor yang dapat mempengaruhi kesalahan manusia dan kerusakan peralatan.
- kerentanan, baik secara individual maupun agregasi
- kontrol yang ada dan seberapa efektif mereka mengurangi kerentanan.

Sebagai contoh, sebuah sistem informasi mungkin memiliki kerentanan terhadap ancaman penyamaran identitas pengguna dan penyalahgunaan sumber daya. Kerentanan penyamaran identitas pengguna mungkin tinggi karena kurangnya otentikasi pengguna. Di sisi lain, kemungkinan penyalahgunaan sumber daya mungkin rendah, meskipun kurangnya otentikasi pengguna, karena terbatasnya cara-cara untuk menyalahgunakan sumber daya.

Tergantung pada kebutuhan untuk ketepatan, aset dapat dikelompokkan, atau mungkin perlu untuk membagi aset ke dalam elemen-elemen mereka dan menghubungkan skenario-skenario pada

elemen tersebut. Sebagai contoh, diberbagai lokasi geografis, sifat ancaman terhadap jenis aset yang sama dapat berubah, atau efektivitas kontrol yang ada dapat bervariasi.

Hasil : Kemungkinan skenario kejadian (kuantitatif atau kualitatif)

8.2.2.4. Tingkat estimasi risiko

Masukan : Sebuah daftar skenario Insiden beserta konsekuensinya terkait dengan aset dan proses bisnis dan kemungkinan mereka (kuantitatif atau kualitatif).

Tindakan : Level risiko harus diperkirakan untuk semua scenarlos insiden yang relevan (berkaitan dengan ISO / IEC 27001, Klausul 4.2.1 e) 4)).

Pedoman pelaksanaan :
Estimasi risiko memberikan nilai untuk kemungkinan dan konsekuensi dari risiko. Nilai-nilai ini mungkin kualitatif atau kuantitatif. Estimasi risiko didasarkan pada konsekuensi dan kemungkinan yang telah dinilai. Selain itu, ia dapat mempertimbangkan manfaat biaya, perhatian pemangku kepentingan, dan variabel lainnya, yang sesuai untuk evaluasi risiko.

Estimasi risiko adalah kombinasi dari kemungkinan skenario insiden dan konsekuensinya.

Contoh metode atau pendekatan risiko keamanan informasi yang berbeda estimasi dapat ditemukan dalam Lampiran E.

Hasil : Sebuah daftar risiko dengan tingkat nilai yang diberikan,

8.3. Evaluasi Risiko

Masukan : Sebuah daftar risiko dengan tingkat nilai yang diberikan dan kriteria evaluasi resiko.

Tindakan : Tingkat risiko harus dibandingkan dengan kriteria evaluasi risiko dan kriteria penerimaan risiko (berkaitan dengan ISO/IEC 27001, Klausul 4.2.1 e) 4)).

Pedoman pelaksanaan :
Sifat dari keputusan yang berkaitan dengan evaluasi risiko dan kriteria evaluasi risiko yang akan digunakan untuk membuat keputusan telah diputuskan ketika menentukan konteks. Keputusan dan konteks ini harus ditinjau kembali secara lebih rinci pada tahap ini ketika telah mengetahui lebih dalam tentang risiko tertentu yang teridentifikasi. Untuk mengevaluasi risiko, organisasi harus membandingkan estimasi risiko (menggunakan metode atau pendekatan yang dipilih seperti dibahas dalam Lampiran E) dengan kriteria evaluasi resiko yang ditentukan selama penentapan konteks.

Kriteria evaluasi risiko yang digunakan untuk membuat keputusan harus konsisten dengan konteks manajemen risiko keamanan informasi eksternal dan internal yang

didefinisikan dan mempertimbangkan tujuan organisasi dan pandangan pemangku kepentingan, dll. Keputusan yang diambil dalam kegiatan evaluasi risiko terutama didasarkan pada level risiko yang dapat diterima. Namun, konsekuensi, kemungkinan, dan tingkat kepercayaan dalam identifikasi dan analisis risiko harus dipertimbangkan juga. Agregasi dari beberapa risiko rendah atau menengah dapat mengakibatkan risiko yang jauh lebih tinggi secara keseluruhan dan perlu karenanya ditangani.

Pertimbangan harus mencakup:

- Sifat keamanan informasi: jika salah satu kriteria tidak relevan bagi organisasi (misalnya hilangnya kerahasiaan), maka semua risiko yang berdampak pada kriteria ini mungkin tidak relevan;
- Pentingnya proses bisnis atau kegiatan yang didukung oleh aset tertentu atau sekumpulan aset: jika proses ditentukan menjadi kepentingan rendah, risiko yang terkait dengan itu diberikan pertimbangan lebih rendah daripada risiko yang berdampak pada proses atau kegiatan yang lebih penting.

Evaluasi Risiko menggunakan pemahaman risiko yang diperoleh dengan analisis risiko untuk membuat keputusan tentang tindakan di masa depan. Keputusan harus mencakup:

1. Apakah kegiatan harus dilakukan
2. Prioritas untuk perlakuan resiko dengan mempertimbangkan estimasi level risiko

Selama tahap evaluasi risiko, persyaratan kontrak, hukum dan peraturan merupakan faktor yang harus diperhitungkan selain risiko-risiko yang telah diperkirakan.

Hasil : Sebuah daftar risiko yang diprioritaskan menurut kriteria evaluasi risiko dalam kaitannya dengan skenario insiden yang mengarah ke risiko tersebut.

9. Penanganan risiko keamanan informasi

9.1. Gambaran umum penanganan risiko

Masukan : Sebuah daftar risiko yang diprioritaskan menurut risiko kriteria evaluasi dalam kaitannya dengan skenario insiden yang mengarah ke risiko tersebut.

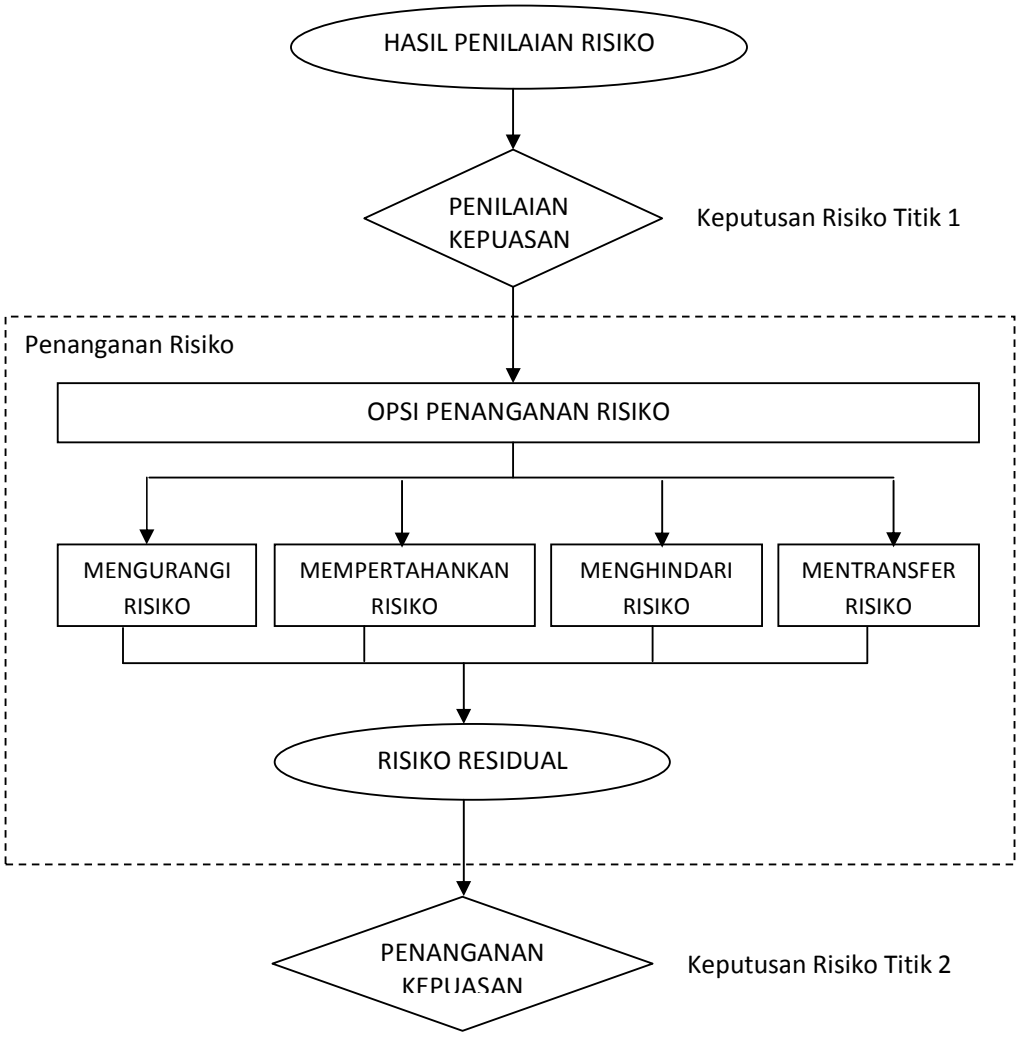
Tindakan : Kontrol untuk mengurangi, mempertahankan, menghindari, atau mentransfer risiko harus dipilih dan rencana penanganan ditetapkan.

Pedoman pelaksanaan :

Ada empat pilihan yang tersedia untuk penanganan risiko: mengurangi risiko (lihat 9.2), mempertahankan risiko (lihat 9.3), menghindari risiko (lihat 9.4) dan mentransfer risiko (lihat 9.5).

CATATAN ISO/IEC 27001 4.2.1. f) 2) menggunakan istilah "menerima resiko" bukan "mempertahankan risiko".

Gambar 2 mengilustrasikan kegiatan penanganan risiko pada proses manajemen risiko keamanan informasi seperti yang disajikan pada Gambar 1.



Gambar 2 - Kegiatan penanganan risiko

Opsi Penanganan Resiko harus dipilih berdasarkan pada hasil penilaian risiko, biaya yang diharapkan untuk menerapkan opsi ini dan manfaat yang diharapkan dari pilihan ini.

Ketika pengurangan besar dalam risiko dapat diperoleh dengan pengeluaran yang relatif rendah, pilihan tersebut harus dilaksanakan. Pilihan selanjutnya untuk perbaikan mungkin tidak ekonomis dan perlu di pertimbangkan, apakah mereka dapat dibenarkan.

Secara umum, konsekuensi risiko yang merugikan harus dibuat serendah yang layak dipraktekkan dan terlepas dari kriteria mutlak. Manajer harus mempertimbangkan resiko yang jarang namun berat. Dalam kasus tersebut, kontrol yang tidak dibenarkan semata-mata atas alasan ekonomi mungkin perlu diterapkan (misalnya, kontrol kelangsungan bisnis dianggap menutupi risiko tinggi tertentu).

Empat opsi untuk penanganan risiko tidak saling eksklusif. Kadang-kadang organisasi bisa mendapatkan keuntungan secara substansial dengan kombinasi pilihan seperti mengurangi kemungkinan risiko, mengurangi konsekuensi mereka, dan mentransfer atau mempertahankan risiko residual.

Beberapa penanganan risiko dapat secara efektif mengatasi lebih dari satu risiko (misalnya pelatihan dan pengetahuan mengenai keamanan informasi). Suatu rencana penanganan risiko harus didefinisikan yang dengan jelas mengidentifikasi urutan prioritas di mana penanganan risiko individu harus dilaksanakan beserta jangka waktunya. Prioritas dapat ditetapkan dengan menggunakan berbagai teknik, termasuk peringkat risiko dan analisis biaya-manfaat. Ini adalah tanggung jawab manajer organisasi untuk menentukan keseimbangan antara biaya penerapan kontrol dan penempatan anggaran.

Identifikasi kontrol yang ada dapat menentukan bahwa kontrol yang ada melebihi kebutuhan saat ini, dalam hal perbandingan biaya. Termasuk pemeliharaan. Jika menghapus kontrol yang berlebihan atau tidak penting dianggap (terutama jika kontrol memiliki biaya pemeliharaan yang tinggi), keamanan informasi dan faktor biaya harus diperhitungkan. Karena kontrol mungkin mempengaruhi satu sama lain, menghapus kontrol berlebihan dapat mengurangi keamanan secara keseluruhan. Selain itu, mungkin lebih murah untuk membiarkan kontrol berlebihan atau tidak perlu daripada menghapusnya.

Opsi penanganan risiko harus dipertimbangkan dengan memperhitungkan:
1. Bagaimana risiko dirasakan oleh pihak-pihak terkait;
2. Cara yang paling tepat untuk berkomunikasi dengan pihak-pihak tersebut.

Penetapan konteks (lihat 7.2 - kriteria evaluasi risiko) memberikan informasi mengenai persyaratan hukum dan peraturan dengan yang perlu dipatuhi oleh organisasi. Risiko bagi organisasi adalah kegagalan untuk mematuhi dan opsi penanganan untuk membatasi kemungkinan ini harus dilaksanakan. Semua kendala - organisasi, teknis, struktural dll - yang diidentifikasikan selama kegiatan penetapan konteks harus diperhitungkan selama penanganan risiko.

Setelah rencana penanganan telah didefinisikan, risiko residual perlu ditentukan. Hal ini melibatkan pembaruan atau perulangan dari penilaian risiko, dengan mempertimbangkan efek yang diharapkan dari penanganan risiko yang diusulkan.

Haruskah risiko residual yang masih belum memenuhi kriteria penerimaan risiko organisasi, iterasi lebih lanjut dari penanganan risiko mungkin diperlukan sebelum melanjutkan ke penerimaan risiko. Informasi lebih lanjut dapat ditemukan di ISO/IEC 27002, Klausul 0.3.

Hasil : rencana penanganan risiko dan risiko residual bergantung pada keputusan penerimaan dari para manajer organisasi.

9.2. Pengurangan risiko

Tindakan : Level risiko harus dikurangi melalui pemilihan kontrol sehingga risiko residual dapat dinilai lagi sebagai risiko yang dapat diterima.

Pedoman pelaksanaan :
Kontrol yang tepat dan dibenarkan harus dipilih untuk memenuhi persyaratan yang diidentifikasi oleh penilaian risiko dan penanganan risiko. Pilihan ini harus mempertimbangkan kriteria penerimaan risiko serta persyaratan hukum, peraturan dan kontrak. Pilihan ini juga harus memperhitungkan biaya dan waktu pelaksanaan kontrol, atau aspek teknis, lingkungan dan budaya. Hal ini sering kali mungkin untuk menurunkan total biaya kepemilikan dari sistem dengan kontrol keamanan informasi yang dipilih secara benar.

Secara umum, kontrol dapat memberikan satu atau lebih dari jenis perlindungan berikut : koreksi, eliminasi, pencegahan, minimalisasi dampak, penolakan, deteksi, pemulihan, pengawasan dan kesadaran. Selama pemilihan kontrol adalah penting untuk mempertimbangkan biaya akuisisi, implementasi, administrasi, operasi, pemantauan, dan pemeliharaan kontrol terhadap nilai aset yang dilindungi. Selanjutnya, laba atas investasi dalam hal pengurangan risiko dan potensi untuk mengeksploitasi peluang bisnis baru yang diberikan oleh kontrol tertentu harus dipertimbangkan. Selain itu, pertimbangan harus diberikan untuk keterampilan khusus yang mungkin diperlukan untuk menentukan dan menerapkan kontrol baru atau memodifikasi yang sudah ada.

ISO/IEC 27002 memberikan informasi rinci tentang kontrol.

Ada banyak kendala yang dapat mempengaruhi pemilihan kontrol. Kendala teknis seperti persyaratan kinerja, pengelolaan (persyaratan dukungan operasional) dan isu kompatibilitas dapat menghambat penggunaan kontrol tertentu atau bisa menyebabkan kesalahan manusia baik meniadakan kontrol, memberikan rasa aman palsu atau bahkan meningkatkan risiko melebihi tidak memiliki kontrol (misalnya mengharuskan *password* yang kompleks tanpa pelatihan yang tepat, sehingga mengarah ke pengguna untuk menuliskan *password*). Selain itu, bisa menjadi kasus bahwa kontrol akan mempengaruhi kinerja. Manajer harus mencoba untuk mengidentifikasi solusi yang memenuhi persyaratan kinerja sembari menjamin keamanan informasi yang memadai. Hasil dari langkah ini adalah daftar kemungkinan kontrol, beserta biaya, manfaat, dan prioritas pelaksanaannya.

Berbagai kendala harus diperhitungkan ketika memilih kontrol dan selama implementasi. Biasanya, mempertimbangkan hal-hal berikut:

1. Kendala waktu
2. Kendala keuangan
3. Kendala teknis
4. Kendala Operasional
5. Kendala kultural
6. Kendala Etis

7. Kendala lingkungan
8. Kendala Hukum
9. Kemudahan penggunaan
10. Kendala Personil
11. Hambatan dalam mengintegrasikan kontrol baru dan yang sudah ada

Informasi lebih lanjut tentang kendala untuk pengurangan risiko dapat ditemukan dalam Lampiran F.

9.3. Retensi risiko

Tindakan : Keputusan mempertahankan risiko tanpa tindakan lebih lanjut harus diambil tergantung pada penilaian risiko.

CATATAN ISO/IEC 27001 4.2.1 f 2) "dengan sengaja dan secara obyektif menerima risiko, asalkan mereka jelas memenuhi kebijakan organisasi dan kriteria untuk menerima risiko" menggambarkan kegiatan yang sama.

Pedoman pelaksanaan :
Jika level risiko memenuhi kriteria penerimaan risiko, tidak perlu menerapkan kontrol tambahan dan risiko dapat dipertahankan.

9.4. Penghindaran risiko

Tindakan : kegiatan atau kondisi yang menimbulkan risiko tertentu harus dihindari.

Pedoman pelaksanaan :
Ketika risiko yang teridentifikasi dianggap terlalu tinggi, atau biaya pelaksanaan pilihan penanganan risiko lain melebihi manfaatnya, keputusan dapat dilakukan untuk menghindari risiko sepenuhnya, dengan membatalkan suatu kegiatan yang direncanakan atau yang sudah ada atau serangkaian kegiatan, atau mengubah kondisi di mana kegiatan tersebut dijalankan. Sebagai contoh, untuk risiko yang disebabkan oleh alam mungkin alternatif yang paling efektif adalah untuk memindahkan fasilitas pengolahan informasi secara fisik ke tempat dimana tidak ada risiko atau berada di bawah kendali.

9.5. Transfer risiko

Tindakan : Risiko harus ditransfer ke pihak lain yang dapat paling efektif mengelola risiko tertentu tergantung pada penilaian risiko.

Pedoman pelaksanaan :
Transfer risiko meliputi keputusan untuk berbagi risiko tertentu dengan pihak eksternal. Transfer risiko dapat menimbulkan resiko baru atau memodifikasi yang sudah ada, mengidentifikasi risiko. Oleh karena itu, penanganan resiko yang mungkin diperlukan.

Transfer risiko dapat dilakukan oleh asuransi yang akan mendukung konsekuensi, atau dengan sub-kontraktor mitra yang perannya akan memonitor sistem informasi dan mengambil tindakan segera untuk menghentikan serangan sebelum membuat tingkat kerusakan yang didefinisikan.

Perlu dicatat bahwa dimungkinkan untuk mengalihkan tanggung jawab untuk mengelola risiko tetapi biasanya tidak mungkin untuk mentransfer tanggung jawab terhadap dampak. Pelanggan biasanya akan menghubungkan dampak buruk sebagai kesalahan dari organisasi.

10. Penerimaan risiko informasi keamanan

Masukan : Rencana penanganan risiko dan subjek penilaian risiko residual untuk keputusan penerimaan para manajer organisasi.

Tindakan : Keputusan untuk menerima risiko dan tanggung jawab terhadap keputusan harus dibuat dan secara resmi dicatat (hal ini berkaitan dengan ISO/IEC 27001 ayat 4.2.1 h)).

Pedoman pelaksanaan :
Rencana penanganan risiko harus menjelaskan bagaimana risiko yang dinilai harus diperlakukan untuk memenuhi kriteria penerimaan risiko (lihat klausul 7.2 kriteria penerimaan risiko). Hal ini penting bagi manajer yang bertanggung jawab untuk meninjau dan menyetujui rencana penanganan risiko yang diusulkan dan mengakibatkan risiko residual, dan mencatat setiap kondisi yang berhubungan dengan persetujuan tersebut.

Kriteria penerimaan risiko dapat lebih kompleks dari sekadar menentukan apakah risiko residual berada di atas atau di bawah ambang tunggal atau tidak.

Dalam beberapa kasus level risiko residual mungkin tidak memenuhi kriteria penerimaan risiko karena kriteria yang diterapkan tidak memperhitungkan keadaan yang berlaku. Sebagai contoh, dapat dikatakan bahwa perlu untuk menerima risiko karena manfaat yang menyertai risiko sangatlah menarik, atau karena biaya pengurangan risiko terlalu tinggi. Keadaan seperti itu menunjukkan bahwa kriteria penerimaan risiko tidak memadai dan harus direvisi jika memungkinkan. Namun, tidak selalu mungkin untuk merevisi kriteria penerimaan risiko secara tepat waktu.

Dalam kasus tersebut, para pembuat keputusan mungkin harus menerima risiko yang tidak memenuhi kriteria penerimaan normal. Jika diperlukan, pembuat keputusan harus mengomentari risiko secara eksplisit dan memasukkan justifikasi atas keputusan untuk mengesampingkan kriteria penerimaan risiko normal.

Hasil : Sebuah daftar risiko yang diterima dengan justifikasi atas risiko-risiko yang tidak memenuhi kriteria penerimaan risiko normal organisasi.

11. Komunikasi risiko keamanan informasi

Masukan : Semua Informasi risiko yang diperoleh dari kegiatan manajemen risiko (lihat Gambar 1).

Tindakan : Informasi tentang risiko harus ditukar dan/atau dibagi antara pembuat keputusan dan pemangku kepentingan lainnya.

Pedoman pelaksanaan :

Komunikasi risiko adalah kegiatan untuk mencapai kesepakatan tentang bagaimana untuk mengelola risiko dengan bertukar dan/atau berbagi informasi tentang risiko antara pengambil keputusan dan pemangku kepentingan lainnya. Informasi meliputi, namun tidak terbatas pada keberadaan, sifat, bentuk, kemungkinan, tingkat kepelikan, penanganan, dan penerimaan risiko.

Komunikasi yang efektif antara para pemangku kepentingan sangat penting karena ini mungkin memiliki dampak yang signifikan terhadap keputusan yang harus dibuat. Komunikasi akan memastikan bahwa mereka yang bertanggung jawab untuk melaksanakan manajemen risiko, dan orang-orang yang memiliki kepentingan pribadi memahami dasar pengambilan keputusan dan mengapa tindakan tertentu yang diperlukan. Komunikasi adalah *bi-directional* (dua arah).

Persepsi risiko dapat bervariasi karena perbedaan asumsi, konsep dan kebutuhan, masalah dan kekhawatiran dari para pemangku kepentingan yang berkaitan dengan risiko atau isu-isu yang sedang dibahas. Stakeholder cenderung membuat penilaian penerimaan risiko berdasarkan persepsi mereka terhadap risiko. Sangat penting untuk memastikan bahwa persepsi para pemangku kepentingan tentang risiko, sama baiknya dengan persepsi mereka tentang keuntungan, dapat diidentifikasi dan didokumentasikan dan alasan yang mendasari dipahami dan ditangani dengan jelas.

Komunikasi risiko harus dilaksanakan untuk mencapai hal-hal berikut:

- Untuk memberikan jaminan hasil manajemen risiko organisasi;
- Untuk mengumpulkan informasi risiko;
- Untuk membagi hasil dari penilaian risiko dan menyampaikan rencana penanganan risiko;
- Untuk menghindari atau mengurangi baik terjadinya maupun konsekuensi dari pelanggaran keamanan informasi karena kurangnya saling pengertian di antara para pembuat keputusan dan pemangku kepentingan;
- Untuk mendukung pengambilan keputusan;
- Untuk mendapatkan pengetahuan baru tentang keamanan informasi;
- Untuk bekerja sama dengan pihak lain dan merencanakan tanggapan untuk mengurangi konsekuensi dari kejadian apapun;
- Untuk memberikan rasa tanggung jawab tentang risiko pada para pembuat keputusan dan pemangku kepentingan;
- Untuk meningkatkan kesadaran.

Sebuah organisasi harus mengembangkan rencana komunikasi risiko untuk operasi normal maupun untuk situasi darurat. Oleh karena itu, kegiatan komunikasi risiko harus dilakukan secara terus menerus.

Koordinasi antara para pengambil keputusan utama dan para pemangku kepentingan dapat dicapai dengan pembentukan sebuah komite di mana perdebatan tentang risiko, prioritas mereka dan penanganan yang tepat, serta penerimaan dapat berlangsung.

Hal ini penting untuk bekerja sama dengan Hubungan Masyarakat yang sesuai atau unit komunikasi dalam organisasi untuk mengkoordinasikan semua tugas yang

berhubungan dengan komunikasi risiko. Ini sangat penting dalam hal tindakan komunikasi krisis, misalnya, dalam menanggapi insiden tertentu.

Hasil : Pemahaman secara terus menerus terhadap proses manajemen risiko keamanan informasi organisasi beserta hasilnya.

12. Pemantauan dan peninjauan risiko keamanan informasi

12.1. Pemantauan dan peninjauan faktor risiko

Masukan : Semua informasi risiko yang diperoleh dari kegiatan manajemen risiko (lihat Gambar 1).

Tindakan : Risiko dan faktor-faktornya (seperti nilai aset, dampak, ancaman, kerentanan, kemungkinan terjadinya) harus dipantau dan dikaji ulang untuk mengidentifikasi perubahan dalam konteks organisasi pada tahap awal, dan untuk menjaga gambaran lengkap keadaan risiko.

Pedoman pelaksanaan :
Resiko tidak statis. Ancaman, kerentanan, kemungkinan atau konsekuensi dapat berubah tiba-tiba tanpa ada indikasi. Oleh karena itu pemantauan konstan diperlukan untuk mendeteksi perubahan ini. Hal ini dapat didukung oleh layanan eksternal yang memberikan informasi mengenai ancaman atau kerentanan baru.

Organisasi harus memastikan bahwa hal-hal berikut ini terus dipantau:

1. Aset baru yang telah dimasukkan dalam lingkup manajemen risiko;
2. Modifikasi diperlukan terhadap nilai aset, misalnya karena perubahan kebutuhan bisnis;
3. Ancaman baru yang bisa aktif baik di luar maupun di dalam organisasi dan yang belum dinilai;
4. Kemungkinan bahwa kerentanan baru atau yang meningkat dapat memungkinkan ancaman untuk mengeksploitasi kerentanan baru atau berubah;
5. Mengidentifikasi kerentanan untuk menentukan mereka yang terekspos sehingga menjadi ancaman baru atau yang muncul kembali;
6. Peningkatan dampak atau konsekuensi dari ancaman, kerentanan dan risiko yang telah dinilai dalam pengumpulan menghasilkan level risiko yang tidak dapat diterima;
7. Insiden keamanan informasi.

Ancaman baru, kerentanan, atau perubahan kemungkinan atau konsekuensi dapat meningkatkan risiko yang telah dinilai sebelumnya sebagai risiko rendah. Tinjauan terhadap risiko yang rendah dan diterima harus memperhitungkan setiap risiko secara terpisah, dan seluruh risiko sebagai suatu kumpulan, untuk menilai akumulasi dampak potensialnya. Jika risiko tidak berada pada kategori risiko terendah yang diterima, risiko itu harus ditangani menggunakan satu atau lebih opsi yang dipertimbangkan dalam Klausul 9.

Faktor-faktor yang mempengaruhi kemungkinan dan konsekuensi terjadinya risiko dapat berubah, seperti faktor-faktor yang mempengaruhi kesesuaian atau

biaya dari berbagai opsi penanganan. Perubahan besar yang mempengaruhi organisasi menjadi alasan untuk tinjauan yang lebih khusus. Oleh karena itu, kegiatan pemantauan risiko harus berulang secara rutin dan opsi penanganan yang dipilih harus ditinjau secara berkala.

Hasil dari kegiatan pemantauan risiko dapat menjadi masukan pada kegiatan peninjauan risiko lain. Organisasi harus meninjau seluruh risiko secara berkala, dan ketika perubahan besar terjadi (menurut ISO/IEC 27001, Klausul 4.2.3)).

Hasil : Manajemen risiko senantiasa selaras dengan tujuan bisnis organisasi, dan kriteria penerimaan risiko.

12.2. Pemantauan, peninjauan dan peningkatan manajemen risiko

Masukan : semua informasi risiko yang diperoleh dari kegiatan manajemen risiko (lihat Gambar 1).

Tindakan : Proses manajemen risiko keamanan informasi harus secara terus menerus dipantau, ditinjau, dan ditingkatkan seperlunya dan dengan tepat.

Pedoman pelaksanaan :
Pemantauan dan peninjauan yang sedang berlangsung sangatlah penting untuk memastikan konteks, hasil dari penilaian risiko dan penanganan risiko, serta rencana pengelolaan, tetap relevan dan sesuai dengan keadaan.

Organisasi harus memastikan bahwa proses manajemen risiko keamanan informasi dan kegiatan terkait tetap sesuai dengan keadaan saat ini dan diikuti. Setiap perbaikan yang disetujui terhadap proses atau tindakan yang perlu untuk meningkatkan kepatuhan pada proses harus diberitahukan kepada manajer yang tepat untuk menjamin bahwa tidak ada risiko atau elemen risiko yang diabaikan atau diremehkan dan bahwa tindakan yang penting telah dilakukan serta keputusan telah dibuat untuk memberikan pemahaman realistis mengenai risiko dan kemampuan untuk menanggapi.

Selain itu, organisasi harus memeriksa secara berkala bahwa kriteria yang digunakan untuk mengukur risiko dan elemen-elemennya masih sah dan konsisten dengan tujuan, strategi dan kebijakan bisnis, dan bahwa perubahan pada konteks bisnia dipertimbangkan secara memadau selama proses manajemen risiko keamanan informasi. Kegiatan pemantauan dan peninjauan harus membahas (tapi tidak terbatas pada):

- Konteks hukum dan lingkungan
- Konteks kompetisi
- Pendekatan penilaian risiko
- Nilai dan kategori aset
- Kriteria dampak
- Kriteria evaluasi risiko
- Kriteria penerimaan risiko
- Total biaya kepemilikan
- Sumber daya yang diperlukan

Organisasi harus memastikan bahwa sumber daya penilaian risiko dan penanganan risiko senantiasa tersedia untuk meninjau risiko, untuk membahas ancaman baru atau perubahan ancaman atau kerentanan, dan untuk memberitahu manajemen sesuai dengan itu.

Pemantauan manajemen risiko dapat mengakibatkan medifikasi atau penambahan pendekatan, metodologi atau peralatan yang digunakan tergantung pada:

1. Perubahan yang diidentifikasi
2. Tujuan dari proses manajemen risiko keamanan rinformasi (seperti kelangsungan bisnis, ketahanan terhadap insiden, kepatuhan)
3. Objek dari proses manajemen risiko keamanan rinformasi (seperti organisasi, unit bisnis, proses informasi, implementasi teknisnya, aplikasi, koneksi ke internet)

Hasil : Relevansi terus-menerus dari proses manajemen risiko keamanan informasi dengan tujuan bisnis organisasi atau memperbarui proses.

LAMPIRAN A
(informatif)
Mendefinisikan ruang lingkup dan batasan dari proses manajemen risiko keamanan informasi

A.1. Studi organisasi

Mengevaluasi organisasi : Studi organisasi mengingat elemen-elemen karakteristik yang mendefinisikan identitas organisasi. Ini menyangkut tujuan, bisnis, misi, nilai-nilai dan strategi organisasi. Hal ini harus diidentifikasi bersama dengan elemen-elemen yang berkontribusi pada pengembangan mereka (seperti subkontrak).

Kesulitan dari kegiatan ini terletak pada pemahaman bagaimana tepatnya organisasi terstruktur. Mengidentifikasi struktur organisasi sebenarnya akan memberikan pemahaman tentang peran dan kepentingan dari masing-masing divisi dalam mencapai tujuan organisasi.

Sebagai contoh, fakta bahwa manajer keamanan informasi melapor kepada manajerpuncak daripada manajer TI mengindikasikan keterlibatan manajer puncak dalam keamanan informasi.

Tujuan utama organisasi : Tujuan utama organisasi dapat didefinisikan sebagai alasan mengapa organisasi tersebut ada (bidang kegiatannya, segmen pasarnya, dll).

Bisnisnya : Bisnis organisasi didefinisikan oleh teknik dan ketrampilan karyawannya, yang memungkinkan untuk mencapai misinya. Hal ini khusus untuk bidang kegiatan organisasi dan seringkali mendefinisikan budaya.

Misinya : Organisasi mencapai tujuannya dengan melakukan misinya. Untuk mengidentifikasi misinya, layanan yang disediakan dan/atau produk yang diproduksi harus diidentifikasi dalam kaitannya dengan pengguna akhir.

Nilainya : Nilai adalah prinsip utama atau kode etik yang terdefinisi diterapkan pada pelaksanaan bisnis.

Ini mungkin mengenai personel, hubungan dengan pihak luar (pelanggan, dll), kualitas produk yang disediakan atau layanan yang diberikan.

Mengambil contoh dari suatu organisasi yang tujuannya adalah layanan publik, yang bisnisnya adalah transportasi dan misinya mencakup membawa anak-anak ke dan dari sekolah. Nilai-nilainya mungkin pada ketepatan waktu dari layanan dan keamanan selama transportasi.

Struktur organisasi . Terdapat berbagai jenis struktur:

- Struktur divisi : setiap divisi ditempatkan dibawah otoritas dari seorang manajer divisi yang bertanggung jawab terhadap keputusan strategis, administratif, dan operasional tentang unitnya.

- Struktur fungsional : otoritas fungsional dijalankan dengan prosedur, sifat pekerjaan, dan kadang-kadang keputusan atau perencanaan (seperti produksi, TI, sumber daya manusia, pemasaran, dll).

Keterangan:

- Suatu divisi dalam organisasi dengan struktu divisi dapat diatur sebagai organisasi berstruktur fungsional dan sebaliknya;
- Organisasi dapat dikatakan memiliki struktur matriks jika memiliki unsur-unsur dari kedua jenis struktur tersebut.
- Dalam setiap struktur organisasi tingkat berikut dapat dibedakan:
    - Tingkat pengambilan keputusan (definisi orientasi strategis);
    - Tingkat kepemimpinan (koordinasi dan manajemen);
    - Tingkat operasional (kegiatan produksi dan dukungan).

Bagan organisasi : struktur organisasi digambarkan secara skematis dalam suatu bagan organisasi. Penggambaran ini harus menyoroti garis pelaporan dan pendelegasian wewenang, tetapi juga harus mencakup hubungan lain, yang, bahkan jika mereka tidak didasarkan pada kekuasaan formal, namun garis arus informasi.

Strategi organisasi : ini memerlukan sebuah ekspresi formal dari prinsip organisasi. Strategi organisasi menentukan arah dan pengembangan yang diperlukan dalam rangka untuk mendapatkan keuntungan dari isu-isu yang dipertaruhkan dan perubahan besar yang direncanakan.

A.2 Daftar kendala yang mempengaruhi organisasi

Semua batasan yang mempengaruhi organisasi dan menentukan orientasi keamanan informasinya harus dipertimbangkan. Sumbernya mungkin berada dalam organisasi dalam hal ini masih dalam kendali mereka atau di luar organisasi dan karena itu umumnya tidak dapat diperbincangkan. Kendala sumber daya (anggaran, personel) dan kendala darurat adalah yang paling penting.

Organisasi menetapkan sasarannya (menyangkut bisnisnya, perilakunya, dll) menyerahkannya pada jalan tertentu, kemungkinan dalam jangka panjang. Hal ini mendefinisikan apa yang diinginkan dan sarana yang perlu diterapkan dalam menentukan jalan ini, organisasi mempertimbangkan pengembangan pada teknik dan ketrampilan, keinginan pengguna, pelanggan, dll. Sasaran ini dapat dinyatakan dalam bentuk strategi atau pengembangan operasi dengan suatu tujuan, sebagai contoh, memangkas biaya operasi, peningkatan kualitas layanan, dll.

Strategi ini mungkin mencakup informasi dan sistem informasi (SI), yang membantu aplikasinya. Akibatnya, karakteristik mengenai identitas, misi, dan strategi organisasi adalah unsur yang mendasar dalam analisa permasalahan karena pelanggaran aspek keamanan informasi dapat menyebabkan pemikiran kembali pada sasaran strategis ini. Selain itu, penting bahwa proposal persyaratan keamanan informasi tetap konsisten dengan aturan, penggunaan, dan sarana yang berlaku dalam organisasi.

Daftar kendala termasuk tetapi tidak terbatas pada:

Kendala yang bersifat politik
Ini mungkin menyangkut administrasi pemerintah, lembaga-lembaga publik atau lebih umumnya setiap organisasi yang harus menerapkan keputusan pemerintah. Mereka biasanya keputusan mengenai strategi atau operasional yang dibuat oleh divisi pemerintah atau badan pembuat keputusan dan harus diterapkan.

Misalnya, komputerisasi faktur atau dokumen administrasi memperkenalkan masalah keamanan informasi.

Kendala yang bersifat strategis
Kendala dapat timbul dari perubahan yang direncanakan atau yang mungkin pada struktur atau orientasi organisasi. Mereka dinyatakan dalam rencana strategis atau operasional organisasi.

Sebagai contoh, kerjasama internasional dalam berbagi informasi yang sensitif memerlukan perjanjian mengenai pertukaran informasi yang aman.

Kendala teritorial
Struktur dan/atau tujuan organisasi memperkenalkan kendala yang spesifik seperti distribusi situs di seluruh wilayah nasional atau luar negeri.

Contoh mencakup layanan pos, kedutaan besar, bank, anak perusahaan dari kelompok industri besar, dll.

Kendala yang timbul dari iklim ekonomi dan politik
suatu pekerjaan organisasi mungkin berubah secara mendalam oleh peristiwa tertentu seperti pemogokan atau krisis nasional dan internasional.

Sebagai contoh, beberapa layanan harus dapat berjalan bahkan selama krisis serius.

Kendala struktural
Sifat dari suatu struktur organisasi (divisi, fungsional atau yang lain) dapat menyebabkan kebijakan keamanan informasi spesifik dan organisasi keamanan disesuaikan dengan struktur.

Sebagai contoh, sebuah struktur internasional harus mampu menyesuaikan persyaratan keamanan khusus untuk tiap negara.

Kendala fungsional
Kendala fungsional timbul secara langsung dari misi organisasi yang bersifat umum atau tertentu.

Sebagai contoh, organisasi yang beroperasi 24 jam sehari harus memastikan sumber dayanya senantiasa tersedia.

Kendala mengenai personel
Sifat dari kendala ini sangat bervariasi. Mereka terkait dengan: tingkat tanggung jawab, perekrutan, kualifikasi, pelatihan, kesadaran tentang keamanan, motivasi, ketersediaan, dll.

Misalnya, seluruh personel dari sebuah organisasi pertahanan harus memiliki otorisasi untuk menangani informasi yang sangat rahasia.

Kendala yang timbul dari kalender organisasi
Kendala ini mungkin hasil dari restrukturisasi atau penataan kebijakan nasional atau internasional baru memaksakan tenggat waktu tertentu.

Sebagai contoh, operasi dari divisi keamanan.

Kendala berkaitan dengan metode
Metode yang sesuai dengan pengetahuan organisasi perlu memaksakan untuk aspek-aspek seperti perencanaan proyek, spesifikasi, pengembangan dan sebagainya.

Misalnya, kendala khas semacam ini perlu menggabungkan kewajiban hukum organisasi dalam kebijakan keamanan.

Kendala yang bersifat budaya
Dalam beberapa organisasi kebiasaan kerja atau bisnis utama telah menyebabkan "budaya" tertentu dalam organisasi, salah satu yang mungkin tidak kompatibel dengan kontrol keamanan. Budaya ini merupakan kerangka acuan umum personel dan dapat ditentukan oleh banyak aspek, termasuk pendidikan, pengajaran, pengalaman profesional, pengalaman luar kerja, pendapat, filosofi, keyakinan, status sosial, dll

Keterbatasan anggaran
Kontrol keamanan yang direkomendasikan kadang memiliki biaya yang sangat tinggi. Meskipun tidak selalu tepat untuk investasi keamanan berbasis efektivitas-biaya, justifikasi ekonomi umumnya diperlukan oleh departemen keuangan organisasi.

Sebagai contoh, di sektor swasta dan beberapa organisasi masyarakat, total biaya dari kontrol keamanan tidak boleh melebihi biaya konsekuensi potensi risiko. Oleh karena itu manajemen puncak harus menilai dan mengambil risiko yang telah diperhitungkan jika mereka ingin menghindari biaya keamanan yang berlebihan.

A.3 Daftar referensi legislatif dan peraturan yang berlaku bagi organisasi

Persyaratan peraturan yang dapat diterapkan pada organisasi harus diidentifikasi. Persyaratan ini boleh jadi hukum, surat keputusan, peraturan khusus dalam bidang organisasi atau peraturan internal/eksternal. Hal ini juga mengenai kontrak dan perjanjian dan lebih umumnya kewajiban yang bersifat hukum atau peraturan.

A.4 Daftar kendala yang mempengaruhi ruang lingkup

Dengan mengidentifikasi kendala dimungkinkan untuk membuat daftar orang-orang yang memiliki dampak pada lingkup dan menentukan mana yang tetap setuju untuk bertindak. Mereka ditambahkan ke, dan mungkin dapat mengubah, kendala organisasi ditentukan di atas. Paragraf berikut menyajikan daftar kemungkinan jenis kendala yang tidak komprehensif.

Kendala yang muncul dari proses yang sudah ada

Proyek aplikasi tidak selalu dikembangkan secara bersamaan. Beberapa proyek bergantung pada proses yang sudah ada. Meskipun satu proses dapat dipecah menjadi sub-proses, proses tidak selalu dipengaruhi oleh semua sub-proses dari proses lain.

Kendala teknis

Kendala teknis, terkait dengan infrastruktur, umumnya timbul dari perangkat keras dan perangkat lunak yang terpasang, dan ruangan atau situs tempat proses.

- Berkas (persyaratan mengenai organisasi, manajemen media, aturan pengelolaan akses, dll);
- Arsitektur umum (persyaratan mengenai topologi (terpusat, distribusi, *client-server*), arsitektur fisik, dll);
- Aplikasi perangkat lunak (persyaratan mengenai desain perangkat lunak tertentu, strandar pasar, dll);
- Paket perangkat lunak (persyaratan mengenai standar, tingkat evaluasi, kualitas, kepatuhan terhadap norma, keamanan, dll);
- Perangkat keras (persyaratan mengenai standar, kualitas, kepatuhan terhadap norma, dll);
- Jaringan komunikasi (persyaratan mengenai jangkauan, standar, kapasitas, keandalan, dll);
- Infrastruktur bangunan (persyaratan mengenai teknik sipil, konstruksi, voltase tinggi, voltase rendah, dll).

Kendala keuangan

Penerapan kontrol keamanan seringkali dibatasi oleh anggaran yang organisasi dapat lakukan.

Namun, kendala keuangan tetap harus menjadi pertimbangan terakhir karena alokasi anggaran untuk keamanan dapat dinegosiasikan berdasarkan studi keamanan.

Kendala lingkungan

Kendala lingkungan timbul dari lingkungan geografis atau ekonomi di mana proses diimplementasikan: negara, iklim, risiko alam, keadaan geografis, iklim ekonomi, dll.

Kendala waktu

Waktu yang diperlukan untuk menerapkan kontrol keamanan harus dipertimbangkan dalam kaitannya dengan kemampuan untuk meningkatkan sistem informasi; jika waktu pelaksanaan sangat panjang, risiko yang kontrolnya dirancang mungkin telah berubah. Waktu adalah faktor yang menentukan untuk memilih solusi dan prioritas.

Kendala berkaitan dengan metode

Metode yang sesuai dengan ketrampilan organisasi harus digunakan untuk perencanaan proyek, spesifikasi, pembangunan dan sebagainya.

Kendala organisasi

Berbagai kendala dapat mengikuti persyaratan organisasi:

- Operasi (persyaratan mengenai *lead-time*, penyediaan jasa, pengawasan, pemantauan, rencana darurat, operasi terdegradasi, dll);

- Pemeliharaan (persyaratan mengenai pemecahan masalah, tindakan preventif, koreksi yang cepat, dll);
- Manajemen sumber daya manusia (persyaratan mengenai penyelenggara dan pelatihan pengguna, kualifikasi untuk posting seperti administrator sistem atau administrator data, dll);
- Manajemen administratif (persyaratan mengenai tanggung jawab, dll);
- Manajemen pengembangan (persyaratan mengenai peralatan pengembangan, rekayasa perangkat lunak, rencana penerimaan, organisasi yang akan dibentuk, dll);
- Manajemen hubungan eksternal (persyaratan mengenai organisasi relasi pihak ketiga, kontrak, dll).

LAMPIRAN B
(informatif)
Identifikasi dan evaluasi penilaian aset dan dampak

B.1. Contoh identifikasi aset

Untuk melakukan evaluasi aset, organisasi perlu mengidentifikasi asetnya terlebih dahulu (pada level rincian yang tepat). Dua jenis aset dapat dibedakan menjadi:

- Aset utama
    - Proses bisnis dan kegiatan
    - Informasi
- Aset pendukung (di mana unsur-unsur utama dari ruang lingkup bergantung) dari semua jenis:
    - Perangkat keras
    - Perangkat lunak
    - Jaringan
    - Personel
    - Tempat
    - Struktur organisasi

B.1.1. Identifikasi aset utama

Untuk menggambarkan ruang lingkup lebih akurat, kegiatan ini terdiri dari mengidentifikasi aset utama (proses bisnis dan kegiatan, informasi). Identifikasi ini dilakukan oleh perwakilan kelompok kerja campuran dari proses (manajer, spesialis sistem informasi dan pengguna).

Aset utama biasanya proses dan informasi inti kegiatan dalam lingkup. Aset utama lainnya seperti proses organisasi juga dapat diperhitungkan, yang akan lebih tepat untuk menyusun kebijakan keamanan informasi atau rencana kelangsungan bisnis. Tergantung pada tujuannya, beberapa studi tidak akan memerlukan analisis mendalam dari semua elemen yang membentuk ruang lingkup. Dalam kasus tersebut, batas-batas penelitian dapat dibatasi pada unsur-unsur kunci dari ruang lingkup.

Aset utama terdiri dari dua jenis:

1. Proses bisnis (atau sub-proses) dan kegiatan, misalnya:
    - Proses yang rugi atau degradasi membuatnya tidak mungkin melaksanakan misi organisasi;
    - Proses yang memuat proses rahasia atau proses yang melibatkan hak paten teknologi;
    - Proses yang, jika dimodifikasi, dapat sangat mempengaruhi pencapaian misi organisasi;
    - Proses yang diperlukan bagi organisasi untuk mematuhi persyaratan kontrak, hukum atau peraturan.
2. Informasi:
   Secara umum, informasi primer terutama terdiri dari:
    - Informasi penting untuk menjalankan misi atau bisnis organisasi;

- Informasi pribadi, seperti dapat didefinisikan secara khusus dalam arti hukum nasional tersebut yang mengenai privasi;
- Informasi strategis yang diperlukan untuk mencapai tujuan ditentukan oleh orientasi strategis;
- Informasi berbiaya tinggi yang pengumpulan, penyimpanan, pemrosesan dan transmisi membutuhkan waktu yang lama dan/atau melibatkan biaya akuisisi yang tinggi.

Proses dan informasi yang tidak didefinisikan sebagai sensitif setelah kegiatan ini akan memiliki klasifikasi pada sisa studi. Hal ini berarti bahwa bahkan jika proses tersebut atau Informasi terganggu, organisasi akan tetap menjalankan misinya dengan sukses.

Namun, mereka akan sering mewarisi kontrol yang dilaksanakan untuk melindungi proses dan informasi yang diidentifikasi sebagai sensitif.

B.1.2. Daftar dan deskripsi dari aset pendukung

Ruang lingkup terdiri dari aset yang harus diidentifikasikan dan dijelaskan. Aset-aset ini mempunyai kerentanan yang dapat dieksploitasi oleh ancaman yang bertujuan untuk merusak aset utama dari ruang lingkup (proses dan informasi). Mereka terdiri berbagai jenis:

Perangkat keras
Jenis perangkat keras terdiri dari semua elemen-elemen fisik yang mendukung proses.

Alat pemroses data (aktif)
Alat untuk memproses informasi secara otomatis termasuk hal yang diperlukan untuk beroperasi secara independen.

Peralatan portabel
Peralatan komputer portabel.

Contoh: laptop komputer, *Personal Digital Assistant* (PDA).

Peralatan tetap
Peralatan komputer yang digunakan di tempat organisasi.

Contoh: *Server*, mikrokomputer yang digunakan sebagai *workstation*.

Pengolah perifer
Peralatan yang terhubung ke komputer melalui *port* komunikasi (serial, hubungan paralel, dll) untuk masuk, menyampaikan atau mengirimkan data.

Contoh: *printer*, *removable disk drive*.

Media data (pasif)
Ini adalah media untuk menyimpan data atau fungsi-fungsi.

Media elektronik
Sebuah media informasi yang dapat dihubungkan ke komputer atau jaringan komputer untuk penyimpanan data.

Meskipun ukurannya yang padat, media ini mungkin berisi sejumlah besar data. Mereka dapat digunakan dengan peralatan komputasi standar.

Contoh: *floppy disk*, *CD ROM*, *back-up cartridge*, *removable harddisk*, *memory key*, *tape*.

Media lain
Statis, media non-elektronik yang berisi data.

Contoh: kertas, *slide*, transparansi, dokumentasi, faks.

Perangkat lunak

Perangkat lunak terdiri dari semua program berkontribusi terhadap pengoperasian perangkat pengolahan data.

Sistem operasi

Ini mencakup semua program komputer yang membentuk basis operasional dari mana semua program lain (sevice atau aplikasi) dijalankan. Ini termasuk kernel dan fungsi atau pelayanan dasar. Tergantung pada arsitektur, sistem operasi mungkin monolitik atau dibuat dari mikro-kernel dan seperangkat layanan sistem. Unsur-unsur utama dari sistem operasi adalah semua peralatan layanan manajemen (CPU, memori, disc, dan antarmuka jaringan), tugas atau proses manajemen layanan dan hak pengguna manajemen layanan.

Layanan, pemeliharaan, atau perangkat lunak administrasi

Sifat perangkat lunak dengan fakta bahwa mereka melengkapi layanan sistem operasi dan tidak langsung pada pelayanan pengguna atau aplikasi (meskipun biasanya penting bahkan sangat diperlukan untuk operasi global sistem informasi).

Perangkat lunak paket atau perangkat lunak standar

Perangkat lunak paket atau perangkat lunak standar adalah produk lengkap yang dikomersialkan seperti itu (satu dari atau pengembangan tertentu) dengan media, rilis, dan pemeliharaan. Mereka menyediakan layanan untuk pengguna atau aplikasi, tapi tidak dikhususkan atau spesifik seperti pada aplikasi bisnis.

Contoh : *data base management software*, *electronic messagin software*, *groupware*, *directory software*, *web server software*, dll.

Aplikasi bisnis

Aplikasi bisnis standar
Ini adalah perangkat lunak komersial yang memberi akses langsung pada layanan atau fungsi kepada pengguna yang diperlukan dari sistem informasi mereka dalam konteks profesional mereka. Terdapat berbagai bidang yang sangat luas, secara teoritis tidak terbatas.

Contoh : *accounts software, software* pengendali peralatan mesin*, customer care software, software* manajemen kompetensi personel*, software* administrasi, dll.

Aplikasi bisnis khusus

Ini adalah perangkat lunak di mana berbagai aspek (terutama dukungan, pemeliharaan, perbaikan, dll) telah dikembangkan secara khusus untuk memberikan akses langsung ke layanan dan fungsi kepada pengguna yang dibutuhkan dari sistem informasi mereka. Terdapat berbagai bidang yang sangat luas, secara teoritis tidak terbatas.

Contoh: manajemen faktur pelanggan operator telekomunikasi, aplikasi pemantauan realtime untuk peluncuran roket.

Jaringan

Jenis jaringan terdiri dari semua perangkat telekomunikasi yang digunakan untuk menghubungkan beberapa komputer yang secara fisik terpencil atau elemen dari suatu sistem informasi.

Media dan dukungan

Media atau peralatan komunikasi dan telekomunikasi ditandai terutama oleh karakteristik peralatan secara fisik dan teknis (link atau jaringan - level 2 dan 3 dari model OSI 7-layer).

Contoh : *Public Switching Telephone Network* (PSTN), *Ethernet*, *GigabitEthernet*, *Asymmetric Digital Subscriber Line* (ADSL), *wireless protocol specifications* (e.g. WiFi 802.11), *Bluetooth*, *FireWire*.

Relai pasif atau aktif

Sub tipe ini termasuk seluruh perangkat yang bukan batasan logis dari komunikasi (visi IS) tapi alat perantara atau relai. Relai dicirikan sebagai protokol pendukung jaringan komunikasi. Selain relai dasar, mereka seringkali memasukkan *routing* dan/atau memfilter fungsi dan layanan, menggunakan komunikasi *switch* dan *router* dengan filer. Mereka sering kali bisa administrasi jarak jauh dan biasanya mampu menghasilkan log.

Contoh : *bridge*, *router*, *hub*, *switch*, pergantian otomatis.

Antarmuka komunikasi

Antarmuka unit pemroses komunikasi terhubung dengan unit pemroses tapi dicirikan oleh media dan protokol pendukung, oleh filter yang terpasang, log, atau fungsi yang menghasilkan peringatan dan kapasitas mereka, dan oleh kemungkinan dan persyaratan dari administrasi jarak jauh.

Contoh : *General Packet Radio Service* (GPRS), adaptor *ethernet.*

Personel

Jenis personel terdiri dari semua kelompok orang yang termasuk dalam sistem informasi.

Pembuat keputusan

Para pembuat keputusan adalah pemilik aset utama (informasi dan fungsi) dan para manajer organisasi atau proyek tertentu.

Contoh : manajemen puncak, pemimpin proyek.

Pengguna

Pengguna adalah personel yang menangani elemen sensitif dalam konteks kegiatan mereka dan mempunyai tanggung jawab khusus dalam hal ini. Mereka mungkin mempunyai hak akses khusus pada sistem informasi untuk melaksanakan tugas harian mereka.

Contoh : manajemen sumber daya manusia, manajemen keuangan, manajer risiko.

Staf operasi/pemeliharaan

Ini adalah personel yang bertanggung jawab atas pengoperasian dan pemeliharaan sistem informasi. Mereka mempunyai hak akses khusus pada sistem informasi untuk melaksanakan tugas harian mereka.

Contoh : administrator sistem, administrator data, *back-up*, *Help Desk*, *application deployment operator*, *security officer*.

Pengembang

Pengembang bertanggung jawab atas pengembangan aplikasi pada organisasi. Mereka mempunyai akses untuk sebagian sistem informasi dengan hak tingkat tinggi tetapi tapi tidak mengambil tindakan apapun pada data produksi.

Contoh : para pengembang aplikasi bisnis.

Situs

Jenis situs terdiri dari semua tempat yang berisi ruang lingkup atau bagian dari ruang lingkup, dan sarana fisik yang diperlukan untuk beroperasi.

Lokasi

Lingkungan eksternal

Ini mengenai semua lokasi dimana sarana keamanan organisasi tidak dapat diterapkan.

Contoh : rumah-rumah personel, tempat dari organisasi lain, lingkungan di luar situs (wilayah perkotaan, wilayah berbahaya)

Tempat

Tempat ini dibatasi oleh perimeter organisasi yang langsung bersentuhan dengan dunia luar. Hal ini mungkin sebuah batasan pelindung fisik yang didapat dari membuat pembatas fisik atau sarana pengawasan disekitar gedung.

Contoh : pendirian gedung.

Zona

Zona dibentuk oleh batas pelindung fisik membentuk partisi dalam bangunan organisasi. Hal ini diperoleh dari membuat pembatas fisik di sekitar infratruktur pemroses informasi organisasi.

Contoh : kantor, zona yang membutuhkan akses , zona aman.

Layanan penting

Semua layanan yang dibutuhkan untuk menjalankan peralatan organisasi.

Komunikasi

Layanan dan peralatan telekomunikasi yang disediakan oleh operator.

Contoh : jalur telepon, PABX, jaringan telepon internal.

Utilitas

Layanan dan sarana (sumber dan pemasangan kawat) diperlukan untuk memberikan daya pada peralatan teknologi informasi dan periferal.

Contoh : tegangan catu daya rendah, *inverter*, rangkaian listrik *head-end.*

Persediaan air

Pembuangan limbah

Layanan dan sarana (peralatan, kontrol) untuk mendinginkan dan memurnikan udara.

Contoh : pipa air dingin, AC.

Organisasi

Jenis organisasi menjelaskan kerangka kerja organisatoris, terdiri dari semua struktur personel yang ditugaskan dan prosedur yang mengontrol struktur ini.

Otoritas

Ini adalah organisasi dari mana organisasi yang dipelajari mendapatkan otoritasnya. Hal itu bisa jadi berafiliasi secara hukum atau eksternal. Hal ini memaksakan batasan pada organisasi yang dipelajari dalam hal peraturan, keputusan dan tindakan.

Contoh : badan pengadministrasian, kantor pusat suatu organisasi.

Struktur organisasi

Terdiri dari berbagai cabang organisasi, termasuk kegiatan lintas fungsi, dibawah kontrol dari manajemennya.

Contoh : manajemen sumber daya manusia, manajemen TI, manajemen pembelian, manajemen unit bisnis, layanan keamanan gedung, layanan kebakaran, manajemen audit.

Proyek atau sistem organisasi

Ini mengenai organisasi yang didirikan untuk proyek atau layanan tertentu.

Contoh : proyek pengembangan aplikasi baru, proyek migrasi sistem informasi.

Subkontraktor/penyedia/produsen
Ini adalah oganisasi yang memberikan layanan atau sumber daya pada suatu organisasi dan terikat dengan kontrak.

B.2. Penilaian Aset

Langkah selanjutnya setelah identifikasi aset adalah untuk menyepakati skala yang akan digunakan dan kriteria untuk menetapkan lokasi tertentu pada skala untuk setiap aset, berdasarkan penilaian. Karena keragaman aset yang ditemukan dalam sebagian besar organisasi ada kemungkinan bahwa beberapa aset yang memiliki nilai moneter yang dikenal akan dihargai di unit lokal dari mata uang sementara yang lain yang memiliki nilai lebih kualitatif dapat diberi nilai mulai, misalnya, dari "sangat rendah" ke "sangat tinggi". Keputusan untuk menggunakan skala kuantitatif versus kualitatif benar-benar masalah preferensi organisasi, tetapi harus relevan dengan aset yang dihargai. Kedua jenis penilaian dapat digunakan untuk aset yang sama.

Istilah yang biasa digunakan untuk penilaian kualitatif aset memuat kata-kata seperti: diabaikan, sangat rendah, rendah, sedang, tinggi, sangat tinggi, dan kritis. Pilihan dan berbagai istilah yang cocok untuk suatu organisasi sangat tergantung pada kebutuhan organisasi terhadap keamanan, ukuran organisasi, dan faktor spesifik organisasi lainnya.

Kriteria
Kriteria yang digunakan sebagai dasar untuk menetapkan nilai untuk setiap aset harus ditulis secara jelas. Sering kali ini adalah salah satu aspek yang paling sulit dari penilaian aset karena nilai beberapa aset mungkin harus ditentukan secara subyektif dan karena banyak individu yang berbeda yang akan membuat ketetapan. Kriteria yang mungkin digunakan untuk menentukan nilai aset meliputi biaya aslinya, penggantian atau biaya penciptaan kembali atau nilainya mungkin abstrak, misalnya nilai reputasi organisasi.

Dasar lain untuk penilaian aset adalah biaya yang timbul akibat hilangnya kerahasiaan, integritas dan ketersediaan karena suatu insiden. Tidak ada penyangkalan, akuntabilitas, keaslian dan keandalan juga harus dipertimbangkan, yang sesuai. Penilaian tersebut akan memberikan dimensi elemen penting untuk nilai aset, selain biaya penggantian, berdasarkan perkiraan konsekuensi bisnis yang merugikan yang akan dihasilkan dari insiden keamanan dengan asumsi set keadaan. Hal ini menekankan bahwa akun pendekatan ini untuk konsekuensi yang diperlukan untuk faktor ke penilaian risiko.

Banyak aset selama penilaian dapat memiliki beberapa nilai yang ditetapkan. Sebagai contoh: rencana bisnis dapat dinilai berdasarkan tenaga kerja yang dikeluarkan untuk mengembangkan rencana, mungkin dihargai pada tenaga kerja untuk input data, dan dapat dinilai berdasarkan nilainya terhadap pesaing. Setiap nilai yang ditetapkan kemungkinan akan berbeda jauh. Nilai yang diberikan mungkin maksimum dari semua nilai yang mungkin atau mungkin jumlah dari beberapa atau semua nilai yang mungkin. Dalam analisis akhir, yang nilai atau nilai-nilai yang ditetapkan untuk aset harus ditentukan secara hati-hati karena nilai akhir yang diberikan masuk ke penentuan sumber daya yang harus dikeluarkan untuk perlindungan aset.

Pengurangan ke dasar umum

Pada akhirnya, semua penilaian aset perlu dikurangi menjadi sebuah dasar umum. Hal ini dapat dilakukan dengan bantuan kriteria seperti mereka yang mengikuti. Kriteria yang dapat digunakan untuk menilai kemungkinan konsekuensi akibat dari hilangnya kerahasiaan, integritas, ketersediaan, tanpa penolakan, akuntabilitas, keaslian, atau keandalan aset adalah:

- Pelanggaran undang-undang dan/atau peraturan
- Penurunan kinerja bisnis
- Hilangnya iktikad baik/efek negatif pada reputasi
- Pelanggaran yang berhubungan dengan informasi pribadi
- Terancamnya keamanan pribadi
- Dampak buruk pada penegakan hukum
- Pelanggaran kerahasiaan
- Pelanggaran atau ketertiban umum
- Kerugian finansial
- Gangguan terhadap kegiatan usaha
- Membahayakan keamanan lingkungan

Pendekatan lain untuk menilai akibatnya antara lain:

- Gangguan terhadap layanan
    - Ketidakmampuan menyediakan layanan
- Hilangnya kepercayaan pelanggan
    - Hilangnya kredibilitas dalam sistem informasi internal
    - Rusaknya reputasi
- Gangguan pada operasi internal
    - Gangguan dalam organisasi itu sendiri
    - Biaya internal tambahan
- Gangguan pada operasi pihak ketiga
    - Gangguan pada transaksi pihak ketiga dengan organisasi
    - Berbagai macam kerusakan
- Pelanggaran hukum/peraturan
    - Ketidakmampuan untuk memenuhi kewajiban hukum
- Pelanggaran terhadap kontrak
    - Ketidakmampuan untuk memenuhi kewajiban kontraktual
- Bahaya bagi keselamatan personel/pengguna
    - Bahaya bagi personel organisasi dan/atau pengguna
- Penyerangan terhadap kehidupan pribadi pengguna
- Kerugian keuangan
- Biaya keuangan untuk darurat atau perbaikan
    - Dalam hal personel,
    - Dalam hal peralatan,
    - Dalam hal studi, laporan ahli.
- Kehilangan barang/dana/aset
- Kehilangan pelanggan, kehilangan pemasok
- Proses peradilan dan hukuman
- Kehilangan keunggulan kompetitif

- Kehilangan teknologi/teknis memimpin
- Kehilangan efektivitas/kepercayaan
- Kehilangan reputasi teknis
- Melemahnya negosiasi kapasitas
- Krisis industri (pemogokan)
- Krisis pemerintah
- Pemberhentian
- Kerusakan material

Kriteria ini adalah contoh masalah yang akan dipertimbangkan untuk penilaian aset. Untuk melakukan penilaian, organisasi perlu untuk memilih kriteria yang relevan dengan jenis usahanya dan persyaratan keamanan. Ini mungkin berarti bahwa beberapa kriteria yang tercantum di atas tidak berlaku, dan bahwa kriteria lain mungkin perlu ditambahkan ke daftar.

Skala

Setelah menetapkan kriteria untuk dipertimbangkan, organisasi harus menyepakati suatu skala untuk digunakan di seluruh organisasi. Langkah pertama adalah memutuskan jumlah tingkatan yang akan digunakan. Tidak ada peraturan sehubungan dengan jumlah tingkatan yang paling sesuai. Lebih banyak tingkatan memberikan tingkat kedalaman data yang lebih baik tapi kadang-kadang diferensiasi terlalu halus membuat tugas yang konsisten di seluruh organisasi menjadi sulit. Biasanya, jumlah tingkatan antara 3 (seperti rendah, sedang, tinggi) dan 10 dapat digunakan selama itu konsisten dengan pendekatan yang digunakan organisasi untuk seluruh proses penilaian risiko.

Suatu organisasi dapat mendefinisikan batasan sendiri untuk nilai aset, seperti 'rendah', 'sedang', atau 'tinggi'. Batasan ini harus dinilai menurut kriteria yang dipilih (misalnya untuk kemungkinan kerugian finansial, harus diberikan nilai moneter, tapi untuk pertimbangan seperti terancamnya keamanan personel, penilaian moneter bisa jadi kompleks dan mungkin tidak sesuai untuk seluruh organisasi). Akhirnya, terserah kepada organisasi untuk memutuskan apa yang diperhitungkan sebagai konsekuensi 'rendah' atau 'tinggi'. Konsekuensi yang mungkin menjadi bencana bagi sebuah organisasi kecil bisa menjadi rendah atau bahkan diabaikan untuk sebuah organisasi yang sangat besar.

Ketergantungan

Semakin relevan dan banyak proses bisnis yang didukung oleh aset, semakin besar nilai aset ini. Dependensi aset pada proses bisnis dan aset lainnya harus diidentifikasi juga karena ini bisa mempengaruhi nilai aset. Sebagai contoh, kerahasiaan data harus dijaga sepanjang siklus hidupnya, di semua tahapan, termasuk penyimpanan dan pengolahan, yaitu kebutuhan keamanan penyimpanan data dan program pengolahan harus langsung berhubungan dengan nilai yang mewakili kerahasiaan data yang disimpan dan diproses. Juga, jika suatu proses bisnis bergantung pada integritas data tertentu yang dihasilkan oleh program, input data dari program ini harus keandalan yang tepat. Selain itu, integritas informasi akan tergantung pada perangkat keras dan perangkat lunak yang digunakan untuk penyimpanan dan pengolahan. Juga, perangkat keras akan tergantung pada pasokan listrik dan mungkin penyejuk udara (AC). Jadi informasi mengenai dependensi akan membantu dalam Identifikasi ancaman dan khususnya kerentanan. Selain itu, ini akan membantu untuk

memastikan bahwa nilai sebenarnya dari aset (melalui hubungan ketergantungan) diberikan kepada aset, sehingga menunjukkan tingkat perlindungan yang sesuai.

Nilai aset dimana aset lain bergantung dapat dimodifikasi dengan cara berikut:

- Jika nilai dari aset yang bergantung (misalnya data) lebih rendah atau sama dengan nilai aset yang diperhitungkan (misalnya perangkat lunak), maka nilainya tetap sama.
- Jika nilai dari aset yang bergantung (misalnya data) lebih tinggi dari nilai aset yang diperhitungkan (misalnya perangkat lunak), maka nilainya harus dinaikkan menurut:
    - Tingkat ketergantungan
    - Nilai dari aset lain

Sebuah organisasi mungkin memiliki beberapa aset yang tersedia lebih dari sekali, seperti salinan program perangkat lunak atau komputer dengan jenis yang sama yang digunakan di sebagian besar kantor. Hal ini penting untuk mempertimbangkan fakta ini ketika melakukan penilaian aset. Di satu sisi, aset tersebut diabaikan dengan mudah, oleh karena itu perawatan harus dilakukan untuk mengidentifikasi mereka semua, di sisi lain, mereka dapat digunakan untuk mengurangi masalah ketersediaan.

Hasil

Hasil akhir dari langkah ini adalah daftar aset dan nilai-nilai mereka relatif terhadap pengungkapan (pemeliharaan kerahasiaan), modifikasi (pemeliharaan integritas, keaslian, tanpa penolakan dan akuntabilitas), tidak tersedia dan perusakan (pemeliharaan ketersediaan dan kehandalan), dan penggantian biaya.

B.3. Penilaian dampak

Insiden keamanan informasi dapat berdampak pada lebih dari satu aset atau hanya sebagian dari satu aset. Dampak berkaitan dengan tingkat kesuksesan insiden. Sebagai konsekuensi, terdapat perbedaan yang penting antara nilai aset dan dampak yang dihasilkan dari insiden. Dampak dianggap memiliki baik efek jangka pendek (operasional) atau efek masa depan (bisnis) yang mencakup konsekuensi keuangan dan pasar.

Dampak jangka pendek (operasional) baik langsung maupun tidak langsung.

Langsung:

a) Nilai penggantian keuangan atas kehilangan (bagian dari) aset
b) Biaya akuisisi, konfigurasi dan instalasi aset baru atau *back-up*
c) Biaya operasi yang ditangguhkan akibat insiden tersebut sampai layanan yang disediakan oleh aset dikembalikan
d) Dampak yang menghasilkan pelanggaran keamanan informasi

Tidak langsung:

a) Biaya peluang (sumber daya keuangan yang diperlukan untuk mengganti atau memperbaiki aset akan telah digunakan di tempat lain)
b) Biaya operasi yang terganggu
c) Penyalahgunaan potensi informasi yang diperoleh melalui pelanggaran keamanan
d) Pelanggaran kewajiban hukum atau peraturan
e) Pelanggaran kode etik

Dengan demikian, penilaian pertama (dengan tidak ada kontrol apapun) akan memperkirakan dampak sebagai sangat dekat dengan (kombinasi) nilai aset yang bersangkutan. Untuk setiap iterasi berikutnya dari aset ini, dampaknya akan berbeda (biasanya jauh lebih rendah) karena kehadiran dan efektivitas kontrol yang diterapkan.

LAMPIRAN C
(informatif)
Contoh ancaman yang khas

Tabel berikut memberikan contoh ancaman yang khas. Daftar ini dapat digunakan selama proses penilaian ancaman. Ancaman mungkin disengaja, tidak disengaja atau lingkungan (alam) dan dapat mengakibatkan, sebagai contoh, pada kerusakan atau kehilangan layanan penting. Daftar berikut menunjukkan untuk setiap jenis ancaman di mana D (disengaja), A (tidak disengaja), E (lingkungan) adalah relevan. D digunakan untuk semua tindakan sengaja ditujukan untuk aset informasi, A digunakan untuk semua tindakan manusia yang tidak sengaja dapat merusak aset informasi, dan E digunakan untuk semua Insiden yang tidak didasarkan pada tindakan manusia. Kelompok-kelompok dari ancaman tidak dalam urutan prioritas.

Tabel 2 - Contoh ancaman yang khas

Jenis	Ancaman	Asal
Kerusakan fisik	Api	A, D, E
	Kerusakan karena air	A, D, E
	Polusi	A, D, E
	Kecelakaan besar	A, D, E
	Perusakan pada peralatan atau media	A, D, E
	Debu, korosi, pembekuan	A, D, E
Peristiwa alam	Fenomena iklim	E
	Fenomena gempa bumi	E
	Fenomena vulkanik	E
	Fenomena meteorologi	E
	Banjir	E
Kehilangan layanan yang penting	Kegagalan AC atau sistem pasokan air	A, D
	Hilangnya pasokan listrik	A, D, E
	Kegagalan peralatan telekomunikasi	A, D
Gangguan akibat radiasi	Radiasi elektromagnetik	A, D, E
	Radiasi panas	A, D, E
	Pulsa elektromagnetik	A, D, E
Kompromi akan informasi	Intersepsi mengorbankan sinyal interferensi	D
	Memata-matai dari jauh	D
	Menguping	D
	Pencurian media atau dokumen	D
	Pencurian peralatan	D
	Retrieval media didaur ulang atau dibuang	
	Penyingkapan	A, D
	Data dari sumber yang tidak dapat dipercaya	A, D
	Gangguan perangkat keras	D
	Gangguan perangkat lunak	A, D
	Pendeteksi posisi	D

Kegagalan teknis	Kegagalan peralatan	A
	Kerusakan peralatan	A
	Kejenuhan sistem informasi	A, D
	Kerusakan perangkat lunak	A
	Pelanggaran pemeliharaan sistem informasi	A, D
Tindakan yang tidak sah	Penggunaan peralatan yang tidak sah	D
	Menyalin perangkat lunak palsu	D
	Penggunaan perangkat lunak palse	A, D
	Korupsi data	D
	Pengolahan data ilegal	D
Kompromi terhadap fungsi	Kesalahan penggunaan	A
	Penyalahgunaan hak	A, D
	Penempaan hak	D
	Penyangkalan pada tindakan	D
	Pelanggaran ketersediaan personel	A, D, E

Perhatian khusus harus diberikan pada sumber ancaman manusia. Tabel berikut adalah sumber ancaman manusia yang telah dirinci secara khusus:

Tabel 3 - Sumber ancaman dari manusia

Asal ancaman	Motivasi	Kemungkinan konsekuensi
Hacker, cracker	Tantangan Ego Pemberontakan Status Uang	- *Hacking* - *Social engineering* - Gangguan sistem, penyusupan - Akses yang tidak sah ke sistem
Kriminal komputer	Perusakan informasi Penyingkapan informasi ilegal Keuntungan moneter Perubahan data yang tidak sah	- Kejahatan komputer (seperti *cyber stalking*) - Tindakan penipuan (mis. *replay*, peniruan, intersepsi) - Informasi suap - *Spoofing* - Intrusi Sistem
Teroris	Pemerasan Perusakan Eksploitasi Balas dendam Keuntungan politik Liputan media	- Bom/terorime - Informasi perang - Serangan sistem (seperti *denial of service* yang disebar) - Penetrasi sistem - Gangguan sistem
Spionase industri (kecerdasan, perusahaan, pemerintah asing,	Keuntungan kompetititf Spionase ekonomi	- Keuntungan pertahanan - Keuntungan politik - Eksploitasi ekonomi - Pencurian informasi

Asal ancaman	Motivasi	Kemungkinan konsekuensi
kepentingan pemerintah lainnya)		- Gangguan pada privasi pribadi - *Social engineering* - Penetrasi sistem - Sistem akses yang tidak sah (akses pada sesuatu yang diklasifikasikan eksklusif, dan/atau informasi terkait teknologi)
Orang dalam (karyawan yang kurang terlatih, tidak puas, berbahaya, lalai, tidak jujur, atau dipecat)	Keuntungan moneter Balas dendam Kesalahan dan kelalaian yang tidak disengaja (seperti kesalahan entri data, kesalahan pemrograman)	- Penyalahgunaan komputer - Kecurangan dan pencurian - Penyuapan informasi - Input dipalsukan, data yang rusak - Penangkapan - Kode berbahaya (misalnya virus, *logic bomb*, *Trojan horse*) - Penjualan informasi pribadi - *Bug* sistem - Intrusi sistem - Sabotase sistem - Sistem akses yang tidak sah

LAMPIRAN D
(informatif)
Kerentanan dan metode untuk penilaian kerentanan

D.1. Contoh kerentanan

Tabel berikut memberikan contoh kerentanan dalam berbagai area keamanan, termasuk contoh ancaman yang mungkin mengeksploitasi kerentanan itu. Daftar ini dapat memberikan bantuan selama penilaian ancaman dan kerentanan, untuk menentukan skenario insiden yang relevan. Ditekankan juga bahwa dalam beberapa kasus ancaman lain dapat mengeksploitasi kerentanan ini.

Tabel 4 - Contoh kerentanan dan ancaman

Jenis	Contoh kerentanan	Contoh ancaman
Perangkat keras	Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan	Pelanggaran pemeliharaan sistem informasi
	Kurangnya skema pergantian berkala	Perusakan peralatan atau media
	Kerentanan terhadap kelembaban, debu, kotoran	Debu, korosi, pendinginan
	Kurangnya kontrol perubahan konfigurasi yang efisien	Kesalahan penggunaan
	Kerentanan terhadap voltase yang bervariasi	Hilangnya pasokan listrik
	Kerentanan terhadap suhu yang bervariasi	Fenomena meteorologis
	Penyimpanan yang tidak dilindungi	Pencurian media atau dokumen
	Kurangnya perawatan di pembuangan	Pencurian media atau dokumen
	Penyalinan yang tidak terkendali	Pencurian media atau dokumen
Perangkat lunak	Tidak ada atau tidak cukup pengujian perangkat lunak	Penyalahgunaan hak
	Kekurangan yang telah diketahui pada perangkat lunak	Penyalahgunaan hak
	Tidak '*logout*' ketika meninggalkan komputer	Penyalahgunaan hak
	Pembuangan atau pemakaian ulang media penyimpanan tanpa penghapusan yang tepat	Penyalahgunaan hak
	Kurangnya *audit trail*	Penyalahgunaan hak
	Kesalahan penempatan hak akses	Penyalahgunaan hak
	Perangkat lunak yang didistribusikan secara luas	Korupsi data
	Menerapkan program aplikasi untuk data yang salah dalam hal waktu	Korupsi data

	Antar muka yang rumit	Kesalahan penggunaan
	Kurangnya dokumentasi	Kesalahan penggunaan
	Kesalahan pengaturan parameter	Kesalahan penggunaan
	Kesalahan tanggal	Kesalahan penggunaan
	Kurangnya mekanisme identifikasi dan otentikasi seperti otentikasi pengguna	Pemalsuan hak
	Tabel *password* yang tidak dilindungi	Pemalsuan hak
	Manajemen *password* yang buruk	Pemalsuan hak
	Layanan yang tidak perlu diaktifkan	Pengolahan data ilegal
	Perangkat lunak baru atau belum matang	Kegagalan perangkat lunak
	Spesifikasi pengembangan yang tidak jelas atau tidak lengkap	Kegagalan perangkat lunak
	Kurangnya kontrol perubahan yang efektif	Kegagalan perangkat lunak
	Pengunduhan dan penggunaan perangkat lunak yang tidak terkontrol	Perusakan dengan perangkat lunak
	Kurangnya salinan *back-up*	Perusakan dengan perangkat lunak
	Kurangnya perlindungan fisik pada gedung, pintu, dan jendela	Pencurian media atau dokumen
	Kesalahan pembuatan laporan manajemen	Penggunaan peralatan yang tidak sah
Jaringan	Kurangnya bukti pengiriman dan penerimaan pesan	Penyangkalan atas tindakan
	Jalur komunikasi yang tidak dilindungi	Menguping
	Lalu lintas sensitif yang tidak dilindungi	Menguping
	Sambungan kabel yang buruk	Kesalahan peralatan komunikasi
	Titik tunggal kegagalan	Kesalahan peralatan komunikasi
	Kurangnya identifikasi dan otentikasi pada pengirim dan penerima	Pemalsuan hak
	Arsitektur jaringan yang tidak aman	*Remote spying*
	Transfer *password* dengan jelas	*Remote spying*
	Manajemen jaringan yang tidak cukup (ketahanan *routing)*	Kejenuhan sistem informasi
	Koneksi jaringan publik yang tidak dilindungi	Penggunaan peralatan yang tidak sah
Personel	Ketidakhadiran personel	Pelanggaran ketersediaan personel
	Prosedur rekrutmen yang tidak cukup	Perusakan peralatan atau media
	Pelatihan keamanan yang tidak cukup	Kesalahan penggunaan
	Kesalahan penggunaan atas perangkat lunak dan perangkat keras	Kesalahan penggunaan

	Kurangnya kesadaran akan keamanan	Kesalahan penggunaan
	Kurangnya mekanisme pemantauan	Pengolahan data ilegal
	Bekerja tanpa pengawasan oleh orang luar atau karyawan pembersih	Pencurian media atau dokumen
	Kurangnya kebijakan untuk penggunaan yang benar atas media telekomunikasi dan pesan	Penggunaan peralatan yang tidak sah
Situs	Penggunaan yang tidak memadai atau ceroboh atas kontrol akses fisik ke bangunan dan ruangan-ruangan	Perusakan peralatan atau media
	Lokasi pada daerah yang rentan banjir	Banjir
	Jaringan listrik yang tidak stabil	Hilangnya pasokan listrik
	Kurangnya perlindungan fisik terhadap gedung, pintu, dan jendela	Pencurian peralatan
Organisasi	Kurangnya prosedur formal untuk pendaftaran dan penghapusan pengguna	Penyalahgunaan hak
	Kurangnya proses formal untuk meninjau hak akses (pengawasan)	Penyalahgunaan hak
	Kurangnya ketentuan yang memadai (mengenai keamanan) dalam kontrak dengan pelanggan dan/atau pihak ketiga	Penyalahgunaan hak
	Kurangnya prosedur pemantauan fasilitas pengolah informasi	Penyalahgunaan hak
	Kurangnya audit berkala (pengawasan)	Penyalahgunaan hak
	Kurangnya prosedur identifikasi dan penilaian risiko	Penyalahgunaan hak
	Kurangnya laporan kesalahan yang tercatat dalam administrator dan pengelola log	Penyalahgunaan hak
	Respon pemeliharaan layanan yang tidak memadai	Menerobos pertahanan sistem informasi
	Kurang atau tidak cukup *Service Level Agreement*	Menerobos pertahanan sistem informasi
	Kurangnya prosedur kontrol perubahan	Menerobos pertahanan sistem informasi
	Kurangnya prosedur formal untuk pengendalian dokumen SMKI	Korupsi data
	Kurangnya prosedur formal untuk rekaman pengawasan SMKI	Korupsi data
	Kurangnya proses formal untuk otorisasi informasi yang tersedia untuk publik	Data dari sumber yang tidak terpercaya
	Kurangnya alokasi yang tepat atas tanggung jawab keamanan informasi	Tindakan penyangkalan
	Kurangnya rencana berkesinambungan	Kerusakan peralatan
	Kurangnya kebijakan penggunaan surat elektronik	Kesalahan penggunaan
	Kurangnya prosedur untuk memperkenalkan perangkat lunak ke dalam	Kesalahan penggunaan

	sistem operasional	
	Kurangnya catatan di administrator dan pengelola log	Kesalahan penggunaan
	Kurangnya prosedur untuk menangani informasi rahasia	Kesalahan penggunaan
	Kurangnya tanggung jawab keamanan informasi dalam deskripsi pekerjaan	Kesalahan penggunaan
	Kurangnya atau tidak memadainya ketentuan (mengenai keamanan informasi) dalam kontrak dengan karyawan	Pengolahan data ilegal
	Kurangnya proses disipliner yang ditetapkan dalam kasus insiden keamanan informasi	Pencurian peralatan
	Kurangnya kebijakan formal pada penggunaan ponsel	Pencurian peralatan
	Kurangnya penguasaan aset lokal	Pencurian peralatan
	Kurangnya atau tidak cukup kebijakan 'meja bersih dan layar bersih'	Pencurian media atau dokumen
	Kurangnya otorisasi fasilitas pengolahan informasi	Pencurian media atau dokumen
	Kurangnya mekanisme pemantauan yang ditetapkan untuk pelanggaran keamanan	Pencurian media atau dokumen
	Kurangnya tinjauan manajemen rutin	Penggunaan peralatan yang tidak sah
	Kurangnya prosedur pelaporan kelemahan keamanan	Penggunaan peralatan yang tidak sah
	Kurangnya prosedur ketentuan sesuai dengan hak intelektual	Penggunaan perangkat lunak palsu atau salinan

D.2 Metode untuk penilaian kerentanan teknis

Metode proaktif seperti pengujian sistem informasi dapat digunakan untuk mengidentifikasi kerentanan tergantung pada kritikalitas dati sistem Teknologi Informasi dan Komunikasi (TIK) dan ketersediaan sumber daya (misalnya alokasi dana, ketersediaan teknologi, orang dengan keahlian untuk melakukan pengujian). Metode pengujian mencakup:

- Alat pemindai kerentanan otomatis
- Pengujian dan evaluasi keamanan
- Pengujian penetrasi
- Peninjauan kode

Alat pemindai kerentanan otomatis digunakan untuk memindai sekelompok *host* atau jaringan untuk layanan yang rentan (seperti sistem yang mengijinkan *File Transfer Protocol* (FTP) anonim, *sendmail relaying*). Perlu dicatat, bagaimanapun, bahwa beberapa potensi kerentanan yang teridentifikasi oleh alat pemindai otomatis mungkin tidak mewakili kerentanan nyata dalam konteks lingkungan sistem. Sebagai contoh, beberapa alat pemindaian menilai kerentanan potensial tanpa mempertimbangkan lingkungan dan persyaratan situs. Beberapa kerentanan yang ditandai oleh perangkat lunak pemindaian

otomatis sebenarnya mungkin tidak rentan untuk situs tertentu, tetapi dapat dikonfigurasi seperti itu karena lingkungan mereka memerlukan itu. Dengan demikian, metode pengujian dapat menghasilkan kerentanan palsu.

Pengujian dan evaluasi keamanan (PEK) adalah teknik lain yang dapat digunakan dalam mengidentifikasi kerentanan sistem TIK selama proses penilaian risiko. Ini termasuk pengembangan dan pelaksanaan rencana uji (misalnya skenario tes, prosedur tes, dan hasil tes yang diharapkan). Tujuan dari pengujian sistem keamanan adalah untuk menguji efektivitas pengendalian keamanan sistem TIK karena mereka telah diterapkan di lingkungan operasional. Tujuannya adalah untuk memastikan bahwa kontrol diterapkan memenuhi spesifikasi keamanan yang disetujui untuk perangkat lunak dan perangkat keras dan menerapkan kebijakan keamanan organisasi atau memenuhi standar industri.

Pengujian penetrasi dapat digunakan untuk melengkapi kajian kontrol keamanan dan memastikan bahwa aspek yang berbeda dari sistem TIK dijamin. Pengujian penetrasi, bila digunakan dalam proses penilaian risiko, dapat digunakan untuk menilai kemampuan sistem TIK untuk menahan upaya yang disengaja untuk menghindari sistem keamanan. Tujuannya adalah untuk menguji sistem TIK dari sudut pandang sumber ancaman dan mengidentifikasi potensi kegagalan dalam skema perlindungan sistem TIK.

Peninjauan kode adalah cara penilaian kerentanan yang paling menyeluruh (tapi juga paling mahal).

Hasil dari jenis pengujian keamanan iniakan membantu mengidentifikasi kerentanan suatu sistem.

Penting untuk dicatat bahwa alat dan teknik penetrasi dapat memberikan hasil yang palsu kecuali kelemahan tersebut berhasil dieksploitasi. Untuk mengeksploitasi kerentanan khusus seseorang harus mengetahui sistem/aplikasi/pengaturan *patch* yang tepat pada sistem yang diuji. Jika data tersebut tidak diketahui pada saat pengujian, mungkin tidak akan berhasil mengeksploitasi kerentanan khusus (misalnya, mendapatkan *remote reverse shell*), namun masih ada kemungkinan untuk *crash* atau *restart* proses atau sistem diuji. Dalam kasus seperti itu, obyek diuji harus dianggap rentan juga.

Metode dapat mencakup kegiatan-kegiatan berikut:

- Wawancara orang dan pengguna
- Kuesioner
- Pemeriksaan fisik
- Analisis dokumen

LAMPIRAN E
(informatif)
Pendekatan penilaian risiko keamanan informasi

E.1. Penilaian risiko keamanan informasi tingkat tinggi

Penilaian tingkat tinggi memungkinkan definisi prioritas dan kronologi dalam tindakan. Untuk berbagai alasan, seperti anggaran, tidak mungkin untuk mengimplementasikan semua kontrol secara bersamaan dan hanya risiko yang paling penting dapat diatasi melalui proses penanganan risiko. Selain itu, bisa jadi belum waktunya untuk memulai manajemen risiko rinci jika pelaksanaannya hanya dipertimbangkan setelah satu atau dua tahun. Untuk mencapai tujuan ini, penilaian tingkat tinggi dapat dimulai dengan penilaian konsekuensi tingkat tinggi bukan dimulai dengan analisis sistematis terhadap ancaman, kerentanan, aset dan konsekuensi.

Alasan lain untuk memulai dengan penilaian tingkat tinggi adalah untuk melakukan sinkronisasi dengan rencana lain terkait dengan manajemen perubahan (atau kelangsungan bisnis). Misalnya, tidak terdengar benar-benar mengamankan sistem atau aplikasi jika direncanakan untuk melakukan *outsourcing* dalam waktu dekat, meskipun masih mungkin layak melakukan penilaian risiko untuk menentukan kontrak *outsourcing*.

Fitur dari iterasi penilaian risiko tingkat tinggi mungkin termasuk yang berikut:

- Penilaian risiko tingkat tinggi dapat menyampaikan pandangan yang lebih global pada organisasi dan sistem informasinya, mempertimbangkan aspek teknologi karena independen dari masalah bisnis. Dengan melakukan ini, analisis konteks lebih berkonsentrasi pada lingkungan bisnis dan operasional dari pada unsur teknologi.
- Penilaian risiko tingkat tinggi dapat menyebutkan daftar ancaman yang lebih terbatas, dan kerentanan dikelompokkan dalam domain yang ditetapkan atau, untuk mempercepat proses, hal ini mungkin fokus pada risiko atau skenario serangan bukan unsur mereka.
- Risiko yang disajikan dalam penilaian risiko tingkat tinggi seringkali domain risiko yang lebih umum daripada risiko yang teridentifikasi spesifik. Karean skenario atau ancaman dikelompokkan dalam domain, penanganan risiko mengusulkan daftar kontrol dalam domain ini. Kegiatan penanganan risiko mencoba kemudian terlebih dahulu mengusulkan dan memilih kontrol umum yang berlaku di seluruh sistem.
- Namun, penilaian risiko tingkat tinggi, karena jarang membahas detail teknologi, lebih tepat untuk memberikan kontrol organisasi dan non-teknis dan aspek manajemen kontrol teknis, atau pengamanan teknis kunci dan umum seperti *back-up* dan anti virus .

Keuntungan dari penilaian risiko tingkat tinggi adalah sebagai berikut:

- Penggabungan pendekatan awal sederhana kemungkinan untuk mendapatkan penerimaan dari program penilaian risiko.
- Ini harus mungkin untuk membangun sebuah gambaran strategis dari program keamanan informasi organisasi, misalnya akan bertindak sebagai alat bantu perencanaan yang baik.

- Sumber daya dan uang dapat diterapkan di mana mereka paling menguntungkan, dan sistem yang paling mungkin membutuhkan perlindungan akan ditangani terlebih dahulu.

Karena analisis risiko awal berada pada tingkat tinggi, dan berpotensi kurang akurat, satu-satunya kelemahan potensial adalah bahwa beberapa proses bisnis atau sistem tidak dapat diidentifikasi karena membutuhkan penilaian risiko rinci kedua. Hal ini dapat dihindari jika ada informasi yang memadai pada semua aspek organisasi dan informasi dan sistemnya, termasuk informasi yang diperoleh dari evaluasi insiden keamanan informasi.

Penilaian risiko tingkat tinggi mempertimbangkan nilai bisnis dari aset informasi, dan risiko dari sudut pandang bisnis organisasi. Pada titik keputusan pertama (lihat Gambar 1), beberapa faktor membantu dalam menentukan apakah penilaian tingkat tinggi cukup untuk menangani resiko, faktor-faktor ini mungkin termasuk yang berikut:

- Sasaran bisnis yang akan dicapai menggunakan berbagai aset informasi;
- Sejauh mana bisnis organisasi tergantung pada setiap aset informasi, yaitu apakah fungsi organisasi menganggap penting untuk kelangsungan hidup atau perilaku yang efektif dari bisnis tergantung pada setiap aset, atau kerahasiaan, integritas, ketersediaan, tanpa penolakan, akuntabilitas, keaslian, dan keandalan informasi yang disimpan dan diproses pada aset ini;
- Tingkat investasi di masing-masing aset informasi, dalam hal mengembangkan, memelihara, atau mengganti aset, dan
- Aset informasi, yang organisasi secara langsung memberikan nilai.

Ketika faktor-faktor ini dinilai, keputusan menjadi lebih mudah. Jika tujuan aset sangat penting untuk melakukan bisnis organisasi, atau jika aset beresiko tinggi, maka iterasi kedua, penilaian risiko rinci, harus dilakukan untuk aset informasi tertentu (atau bagian daripadanya).

Aturan umum untuk menerapkan adalah jika kekurangan keamanan informasi dapat mengakibatkan konsekuensi merugikan yang signifikan terhadap organisasi, proses bisnis atau aset-asetnya, maka penilaian risiko iterasi kedua, pada tingkat yang lebih rinci, perlu untuk mengidentifikasi potensi risiko.

E.2. Penilaian risiko keamanan informasi terperinci

Proses penilaian risiko keamanan informasi terperinci melibatkan identifikasi dan penilaian mendalam pada aset, penilaian ancaman terhadap aset tersebut, dan penilaian kerentanan. Hasil dari kegiatan ini kemudian digunakan untuk menilai risiko dan kemudian mengidentifikasi penanganan risiko.

Langkah rinci biasanya membutuhkan waktu, usaha dan keahlian, dan karena itu mungkin yang paling cocok untuk sistem informasi yang berisiko tinggi.

Tahap akhir dari penilaian risiko keamanan informasi rinci untuk menilai keseluruhan risiko, yang merupakan fokus dari lampiran ini.

Konsekuensi dapat dinilai dalam beberapa cara, termasuk menggunakan kuantitatif, misalnya moneter, dan langkah-langkah kualitatif (yang dapat didasarkan pada penggunaan

kata sifat seperti sedang atau berat), atau kombinasi keduanya. Untuk menilai kemungkinan terjadinya ancaman, kerangka waktu di mana aset akan memiliki nilai atau kebutuhan untuk dilindungi harus ditetapkan. Kemungkinan suatu terjadi secara ancaman spesifik dipengaruhi oleh hal-hal berikut:

- Daya tarik aset, atau dampak yang mungkin juga berlaku di saat ancaman manusia yang disengaja sedang dipertimbangkan;
- Kemudahan konversi mengeksploitasi kerentanan aset menjadi hadiah, berlaku jika ancaman manusia yang disengaja sedang dipertimbangkan;
- Kemampuan teknis dari agen ancaman, berlaku untuk ancaman manusia yang disengaja, dan
- Kelemahan dari kerentanan terhadap eksploitasi, berlaku untuk kerentanan baik teknis dan non-teknis.

Banyak metode menggunakan tabel, dan menggabungkan ukuran subjektif dan empiris. Suatu hal penting bahwa organisasi menggunakan metode dengan mana organisasi ini menjadi nyaman, di mana organisasi memiliki kepercayaan diri, dan yang akan menghasilkan hasil yang berulang. Beberapa contoh teknik berbasis tabel diberikan di bawah ini.

E.2.1. Contoh 1 Matriks dengan nilai-nilai yang telah ditetapkan

Dalam metode penilaian risiko jenis ini, aset fisik yang sebenarnya atau yang diusulkan dinilai dalam hal biaya penggantian atau rekonstruksi (yaitu pengukuran kuantitatif). Biaya tersebut kemudian dikonversi ke skala kualitatif sama dengan yang digunakan untuk informasi (lihat di bawah). Aset perangkat lunak yang sebenarnya atau yang diusulkan dinilai dalam cara yang sama seperti aset fisik, dengan biaya pembelian atau rekonstruksi diidentifikasi dan kemudian diubah dengan skala kualitatif sama dengan yang digunakan untuk mendapatkan informasi. Selain itu, jika ada perangkat lunak aplikasi yang ditemukan memiliki persyaratan intrinsik sendiri untuk kerahasiaan atau integritas (misalnya jika *source code* itu sendiri sensitif secara komersial), itu dihargai dengan cara yang sama seperti untuk informasi.

Nilai-nilai informasi yang diperoleh dengan mewawancarai manajemen bisnis yang dipilih ("pemilik data ") yang dapat berbicara secara otoriter tentang data, untuk menentukan nilai dan sensitivitas data sebenarnya yang digunakan, atau untuk disimpan, diproses atau diakses. Wawancara memfasilitasi penilaian nilai dan sensitivitas informasi dalam hal skenario terburuk yang bisa diduga akan terjadi dari konsekuensi bisnis yang merugikan karena pengungkapan yang tidak sah, modifikasi yang tidak sah, tidak tersedia pada berbagai periode waktu, dan kehancuran.

Penilaian ini dilakukan dengan menggunakan pedoman penilaian informasi, yang meliputi isu-isu seperti:

- Keamanan pribadi
- Informasi pribadi
- Kewajiban hukum dan peraturan
- Penegakan hukum
- Kepentingan komersial dan ekonomi
- Kerugian finansial/terganggunya kegiatan

- Ketertiban umum
- Kebijakan dan operasi bisnis
- Kehilangan niat baik
- Kontrak atau perjanjian dengan pelanggan

Pedoman ini memfasilitasi identifikasi nilai-nilai pada skala numerik, seperti 0 sampai 4 skala ditunjukkan dalam contoh matriks di bawah ini, sehingga memungkinkan pengakuan nilai kuantitatif yang mungkin dan logis, dan nilai-nilai kualitatif jika nilai-nilai kuantitatif tidak mungkin, misalnya untuk membahayakan kehidupan manusia.

Kegiatan utama berikutnya adalah penyelesaian pasangan kuesioner untuk setiap jenis ancaman, untuk setiap pengelompokan aset dimana jenis ancaman berkaitan dengan, untuk memungkinkan penilaian tingkat ancaman (kemungkinan terjadinya) dan tingkat kerentanan (kemudahan eksploitasi oleh ancaman menyebabkan konsekuensi yang merugikan). Setiap jawaban pertanyaan menarik skor. Skor ini terakumulasi melalui basis pengetahuan dan dibandingkan dengan rentang. Ini mengidentifikasi tingkat ancaman dalam mengatakan skala tinggi sampai rendah dan tingkat kerentanan yang sama, seperti yang ditunjukkan pada contoh matriks di bawah ini, membedakan antara jenis konsekuensi sebagai relevan. Informasi untuk menyelesaikan kuesioner harus dikumpulkan dari wawancara dengan orang teknis, orang personalia dan orang akomodasi yang tepat, dan inspeksi lokasi fisik, dan tinjauan dokumentasi.

Nilai aset, dan tingkat ancaman dan kerentanan, relevan untuk setiap jenis konsekuensi, dicocokkan dalam matriks seperti yang ditunjukkan di bawah ini, untuk mengidentifikasi setiap kombinasi ukuran risiko yang relevan pada skala 0 sampai 8. Nilai-nilai ditempatkan dalam matriks dengan cara yang terstruktur. Sebuah contoh diberikan di bawah ini:

Tabel 5 - Matriks nilai aset, kemungkinan terjadi, dan kemudahan eksploitasi

	Kemungkinan terjadi - Ancaman	Rendah (R)			Sedang (S)			Tinggi (T)		
	Kemudahan eksploitasi	R	S	T	R	S	T	R	S	T
Nilai aset	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Untuk setiap aset, kerentanan dan ancaman yang relevan dipertimbangkan. Jika ada kerentanan tanpa ancaman yang sesuai, atau ancaman tanpa kerentanan yang sesuai, saat ini belum ada risiko (tetapi perawatan harus dilakukan seandainya situasi ini berubah). Adapun baris yang sesuai dalam matriks diidentifikasi oleh nilai aset, dan kolom yang sesuai diidentifikasi oleh kemungkinan terjadinya ancaman dan kemudahan eksploitasi. Sebagai contoh, jika aset memiliki nilai 3, ancamannya adalah "tinggi" dan kerentanan "rendah", maka ukuran risiko adalah 5. Asumsikan aset memiliki nilai 2, misalnya untuk modifikasi, tingkat ancaman "rendah" dan kemudahan eksploitasi adalah "tinggi", maka ukuran risiko adalah 4. Ukuran matriks, dalam hal jumlah kategori kemungkinan ancaman, kategori

kemudahan eksploitasi dan jumlah kategori penilaian aset, bisa disesuaikan dengan kebutuhan organisasi. Kolom dan baris tambahan akan mengharuskan ukuran risiko tambahan. Nilai dari pendekatan ini adalah dalam peringkat risiko yang harus ditangani.
Sebuah matriks yang sama seperti yang ditunjukkan pada Tabel 6 hasil dari pertimbangan kemungkinan skenario insiden, dipetakan terhadap dampak bisnis diperkirakan. Kemungkinan skenario insiden diberikan oleh ancaman yang mengeksploitasi kerentanan dengan kemungkinan tertentu. Tabel memetakan kemungkinan ini terhadap dampak bisnis yang terkait dengan skenario insiden. Risiko yang timbul diukur pada skala 0 sampai 8 yang dapat dievaluasi terhadap kriteria penerimaan risiko. Skala risiko ini juga bisa dipetakan ke peringkat risiko keseluruhan yang sederhana, misalnya seperti:

- Resiko rendah: 0-2
- Medium Risk: 3-5
- Risiko Tinggi :6-8

Tabel 6 - Matriks kemungkinan skenario insiden dan dampak bisnis

	Kemungkinan skenario insiden	Sangat rendah (sangat tidak mungkin)	Rendah (tidak mungkin)	Sedang (mungkin)	Tinggi (mungkin sekali)	Sangat tinggi (sering)
Dampak bisnis	Sangat rendah	0	1	2	3	4
	Rendah	1	2	3	4	5
	Sedang	2	3	4	5	6
	Tinggi	3	4	5	6	7
	Sangat tinggi	4	5	6	7	8

E.2.2. Contoh 2 Peringkat ancaman dengan pengukuran risiko

Matriks atau tabel seperti yang ditunjukkan pada Tabel 7 dapat digunakan untuk menghubungkan faktor konsekuensi (nilai aset) dan kemungkinan terjadinya ancaman (mempertimbangkan aspek kerentanan). Langkah pertama adalah mengevaluasi konsekuensi (nilai aset) pada skala yang terdefinisi, misalny 1 sampai 5, dari setiap aset yang terancam (kolom "b" dalam tabel). Langkah kedua adalah mengevaluasi kemungkinan terjadinya ancaman pada skala yang terdefinisi, misalnya 1 sampai 5, dari setiap ancaman (kolom "c" dalam tabel). Langkah ketiga adalah menghitung ukuran risiko dengan mengkalikan (b x c). Akhirnya ancaman dapat diurutkan dalam rangka mengukur risiko mereka. Perhatikan bahwa dalam contoh ini, 1 diambil sebagai konsekuensi terendah dan kemungkinan terjadi yang terendah.

Tabel 7 - Matriks ancaman

Deskripsi ancaman (a)	Nilai konsekuensi (aset) (b)	Kemungkinan terjadinya ancaman (c)	Ukuran risiko (d)	Urutan ancaman (e)
Ancaman A	5	2	10	2
Ancaman B	2	4	8	3
Ancaman C	3	5	15	1
Ancaman D	1	3	3	5
Ancaman E	4	1	4	4
Ancaman F	2	4	8	3

Seperti ditunjukkan di atas, ini adalah prosedur yang memungkinkan ancaman yang berbeda dengan konsekuensi dan kemungkinan terjadinya yang berbeda harus dibandingkan dan diperingkat dalam urutan prioritas, seperti yang ditunjukkan di sini. Dalam beberapa kasus akan diperlukan untuk mengaitkan nilai uang dengan skala empiris digunakan di sini.

E.2.3. Contoh 3 Menilai nilai untuk kemungkinan dan konsekuensi risiko

Dalam contoh ini, penekanannya ditempatkan pada konsekuensi insiden keamanan informasi (yaitu, skenario insiden) dan menentukan sistem harus diberikan prioritas. Hal ini dilakukan dengan menilai dua nilai untuk masing-masing aset dan risiko, yang dalam kombinasi akan menentukan skor untuk setiap aset. Ketika semua nilai aset untuk sistem dijumlahkan, ukuran rlsk ke sistem yang ditentukan.

Pertama, nilai yang ditetapkan untuk masing-masing aset. Nilai ini berkaitan dengan konsekuensi yang berpotensi merugikan yang dapat timbul jika aset tersebut terancam. Untuk setiap ancaman yang berlaku pada aset, nilai aset ini ditetapkan untuk aset.

Selanjutnya nilai kemungkinan dinilai. Hal ini dinilai dari kombinasi kemungkinan ancaman yang terjadi dan kemudahan eksploitasi kerentanan, lihat Tabel 8 mengungkapkan kemungkinan skenario insiden.

Tabel 8 - Nilai kemungkinan skenario risiko

Kemungkinan ancaman	Rendah (R)			Sedang (S)			Tinggi (T)		
Level kerentanan	R	S	T	R	S	T	R	S	T
Nilai kemungkinan dari skenario insiden	0	1	2	1	2	3	2	3	4

Selanjutnya, skor aset /ancaman ditetapkan dengan menemukan persimpangan nilai aset dan nilai kemungkinan dalam Tabel 9. Skor aset/ancaman dijumlahkan untuk menghasilkan skor total aset. Angka ini dapat digunakan untuk membedakan antara aset yang membentuk bagian dari sistem.

Tabel 9 - Matriks nilai aset dan nilai kemungkinan

Nilai aset	0	1	2	3	4
Nilai kemungkinan					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Langkah terakhir adalah menjumlah semua nilai total aset untuk aset dari sistem, menghasilkan skor sistem. Ini dapat digunakan untuk membedakan antara sistem dan untuk menentukan perlindungan sistem harus diberi prioritas.

Dalam contoh berikut semua nilai dipilih secara acak.

Misalkan Sistem S memiliki tiga aset A1, A2, dan A3. Juga misalkan ada dua ancaman T1 dan T2 berlaku untuk sistem S. Biarkan nilai A1 menjadi 3, demikian juga biarkan nilai aset A2 menjadi 2 dan nilai aset A3 menjadi 4.

Jika untuk A1 dan T1 kemungkinan ancaman rendah dan kemudahan eksploitasi kerentanan adalah sedang, maka nilai kemungkinan adalah 1 (lihat Tabel E.3).

Skor aset/ancaman A1/T1 dapat diturunkan dari Tabel E.4 sebagai persimpangan nilai aset 3 dan nilai kemungkinan 1, yaitu 4. Demikian pula, untuk A1/T2 biarkan kemungkinan ancaman adalah sedang dan kemudahan eksploitasi kerentanan yang tinggi, memberikan nilai A1/T2 dari 6.

Adapun total skor aset A1T dapat dihitung, yaitu 10. Total skor aset dihitung untuk setiap aset dan ancaman yang berlaku. Total skor sistem dihitung dengan menambahkan A1T + + A2T A3T untuk memberikan ST.

Adapun sistem yang berbeda dapat dibandingkan dengan menetapkan prioritas dan aset yang berbeda dalam satu sistem juga.

Contoh di atas menunjukkan dalam hal sistem informasi, namun pendekatan serupa dapat diterapkan pada proses bisnis.

LAMPIRAN F
(informatif)
Kendala untuk pengurangan risiko

Sembari mempertimbangkan kendala untuk pengurangan risiko, kendala berikut harus diperhitungkan:

Kendala waktu:
Banyak jenis kendala waktu bisa dijumpai. Misalnya, kontrol harus dilaksanakan dalam jangka waktu yang dapat diterima bagi para manajer organisasi. Tipe lain dari kendala waktu adalah apakah kontrol dapat diimplementasikan dalam masa informasi atau sistem. Jenis ketiga dari kendala waktu mungkin periode waktu yang diputuskan para manajer organisasi merupakan periode diterima untuk risiko tertentu.

Kendala keuangan:
Kontrol tidak boleh lebih mahal untuk dilaksanakan atau untuk dipertahankan dari nilai risiko yang mereka rancang untuk dilindungi, kecuali kepatuhan wajib (misalnya dengan undang-undang). Setiap upaya harus dilakukan untuk tidak melebihi anggaran yang ditetapkan dan mencapai keuntungan finansial melalui penggunaan kontrol. Namun, dalam beberapa kasus tidak mungkin untuk mencapai keamanan dan tingkat penerimaan risiko yang diinginkan karena keterbatasan anggaran. Dikarenakan itu menjadi keputusan para manajer organisasi untuk resolusi situasi ini.

Harus diwaspadai jika anggaran mengurangi jumlah atau kualitas kontrol untuk dilaksanakan karena hal ini dapat menyebabkan retensi implisit risiko yang lebih besar dari yang direncanakan. Anggaran yang ditetapkan untuk kontrol seharusnya hanya digunakan sebagai faktor pembatas dengan perhatian yang cukup.

Kendala teknis:
Masalah teknis, seperti kompatibilitas program atau perangkat keras, dengan mudah dapat dihindari jika mereka diperhitungkan dalam pemilihan kontrol. Selain itu, penerapan retrospektif kontrol untuk proses atau sistem yang ada sering terhambat oleh kendala teknis. Kesulitan-kesulitan ini dapat memindahkan keseimbangan kontrol terhadap aspek keamanan yang bersifat prosedural dan fisik. Mungkin perlu untuk merevisi program keamanan informasi dalam rangka mencapai tujuan keamanan. Hal ini dapat terjadi ketika kontrol tidak memenuhi hasil yang diharapkan dalam mengurangi risiko tanpa mengurangi produktivitas.

Kendala operasional:
Kendala operasional seperti kebutuhan untuk beroperasi 24x7 namun masih melakukan *back-up* dapat mengakibatkan implementasi kontrol yang kompleks dan mahal kecuali mereka dibangun ke dalam desain dari awal.

Kendala kultural:
Kendala budaya untuk pemilihan kontrol mungkin khusus untuk suatu negara, sektor, organisasi atau bahkan departemen dalam suatu organisasi. Tidak semua kontrol dapat diterapkan di semua negara. Sebagai contoh, dimungkinkan untuk melaksanakan pencarian tas di beberapa bagian Eropa tetapi tidak di bagian Timur Tengah. Aspek budaya tidak dapat diabaikan karena banyak kontrol bergantung pada dukungan aktif dari staf. Jika staf

tidak memahami perlunya kontrol atau tidak diterima secara budaya, kontrol akan menjadi tidak efektif dari waktu ke waktu.

Kendala Etika:
Kendala etika dapat memiliki implikasi besar pada kontrol karena etika berubah berdasarkan norma-norma sosial. Hal ini dapat mencegah penerapan kontrol seperti *email scanning* di beberapa negara. Kerahasiaan informasi juga dapat berubah tergantung pada etika daerah atau pemerintah. Ini mungkin menjadi perhatian lebih di beberapa sektor industri daripada yang lain, misalnya, pemerintahan dan kesehatan.

Kendala lingkungan:
Faktor-faktor lingkungan dapat mempengaruhi pemilihan kontrol, seperti ketersediaan ruang, kondisi iklim yang ekstrim, geografi alam dan perkotaan. Misalnya pemeriksaan gempa mungkin diperlukan di beberapa negara tapi tidak perlu pada negara lain.

Kendala hukum:
Faktor hukum seperti perlindungan data pribadi atau ketentuan hukum pidana untuk memproses informasi dapat mempengaruhi pemilihan kontrol. Kepatuhan legislatif dan peraturan dapat mengamanatkan jenis kontrol tertentu termasuk perlindungan data dan audit keuangan, mereka juga dapat mencegah penggunaan beberapa kontrol, misalnya enkripsi. Hukum dan peraturan lain seperti undang-undang hubungan kerja, pemadam kebakaran, kesehatan dan keselamatan, dan peraturan sektor ekonomi, dll., bisa mempengaruhi pemilihan kontrol juga.

Mudah digunakan:
Sebuah antarmuka manusia-teknologi yang buruk akan menghasilkan kesalahan manusia dan dapat membuat kontrol tidak berguna. Kontrol harus dipilih untuk memberikan kemudahan penggunaan optimal sembari mencapai tingkat risiko residual yang dapat diterima untuk bisnis. Kontrol yang sulit untuk digunakan akan berdampak pada efektivitas mereka, karena pengguna dapat mencoba untuk menghindari atau mengabaikan mereka sebanyak mungkin. Kontrol akses yang kompleks dalam suatu organisasi dapat mendorong pengguna untuk menemukan alternatif, metode yang tidak sah akses.

Personil kendala:
Ketersediaan dan biaya gaji dari keahlian khusus ditetapkan untuk menerapkan kontrol, dan kemampuan untuk memindahkan staf antara lokasi dalam kondisi operasi yang merugikan, harus dipertimbangkan. Keahlian mungkin tidak tersedia untuk menerapkan kontrol yang direncanakan atau keahlian mungkin terlalu mahal bagi organisasi. Aspek lain seperti kecenderungan beberapa staf untuk membedakan anggota staf lain yang tidak diperiksa keamanan memiliki implikasi besar bagi kebijakan dan praktik keamanan. Selain itu, kebutuhan untuk mempekerjakan orang yang tepat untuk pekerjaan, dan menemukan orang yang tepat, dapat mengakibatkan mempekerjakan sebelum pemeriksaan keamanan. Apakah selesai. Persyaratan untuk pemeriksaan keamanan akan selesai sebelum menyewa adalah normal, dan paling aman, praktek.

Kendala mengintegrasikan kontrol baru dan yang sudah ada:
Integrasi kontrol baru dalam infrastruktur yang ada dan saling ketergantungan antara kontrol sering diabaikan. Kontrol baru mungkin tidak mudah dilaksanakan jika ada keganjilan atau ketidakcocokan dengan kontrol yang ada. Misalnya, rencana untuk menggunakan token

biometrik untuk kontrol akses fisik dapat menyebabkan konflik dengan sistem berbasis PIN-pad yang ada untuk kontrol akses. Biaya perubahan kontrol dari kontrol yang ada dengan kontrol yang direncanakan harus mencakup elemen yang akan ditambahkan pada biaya keseluruhan penanganan risiko. Mungkin tidak bisa menerapkan kontrol yang dipilih karena gangguan dengan kontrol saat ini.

Bibliografi

[1] ISO/IEC *Guide* 73:2002, *Risk management - Vocabulary - Guidelines for use in standards*

[2] ISO/IEC 16085:2006, *Systems and software engineering - Life cycle processes - Risk management*

[3] AS/NZS 4360:2004, *Risk Management*

[4] *NIST Special Publication* 800-12, *An Introduction to Computer Security*: *The NIST Handbook*

[5] *NIST Special Publication* 800-30, *Risk Management Guide for Information Technology Systems*,

[6] *Recommendations of the National Institute of Standards and Technology*