APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

MANAJEMEN KEAMANAN INFORMASI DAN INTERNET

Topik Bahasan

SEPULUH ASPEK KEAMANAN DALAM STANDAR INTERNASIONAL

Versi

2013/1.0

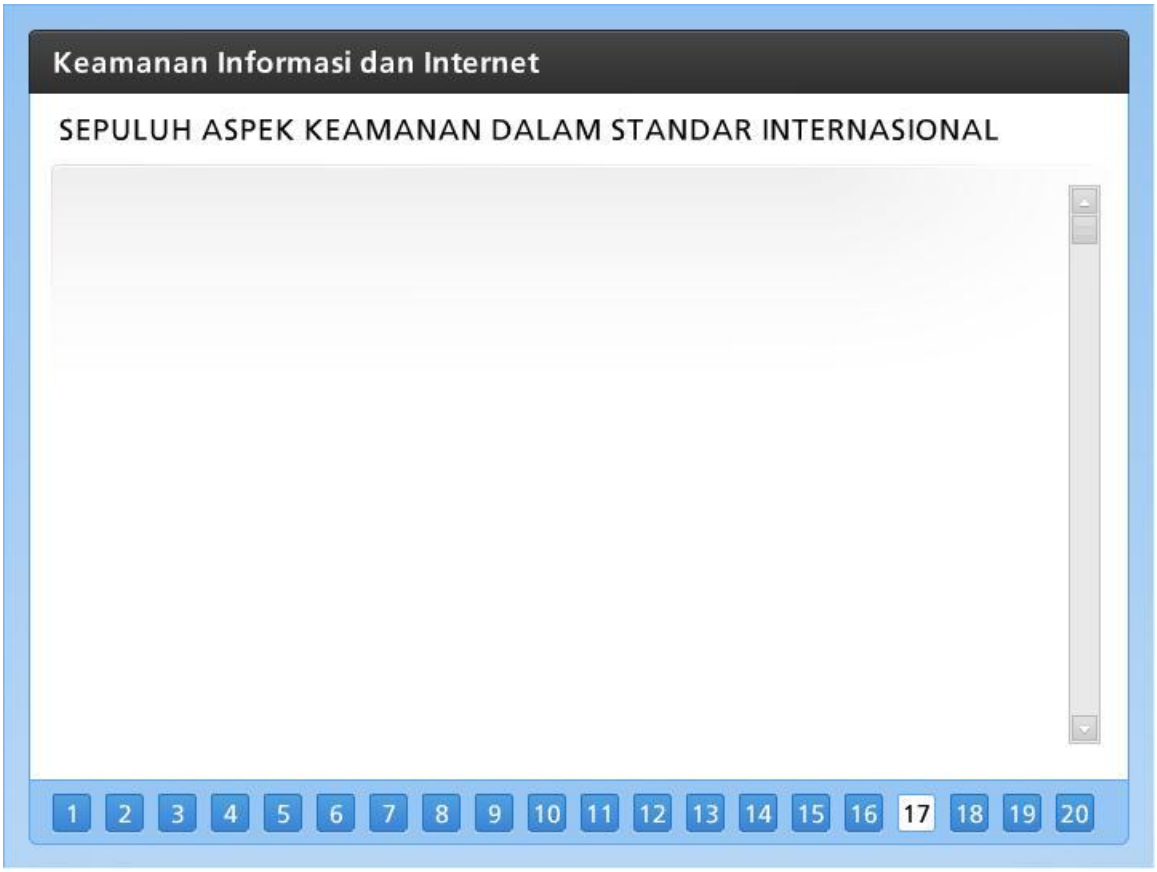
Nama File

MKIDI-3B-SepuluhAspek.pdf

Referensi Pembelajaran

3-B

SEPULUH ASPEK KEAMANAN DALAM STANDAR INTERNASIONAL



Pendahuluan

ISO (the International Organization for Standarization) dan IEC (the International Electrotechnical Commission) membentuk sistem khusus untuk standardisasi universal. Badan-badan nasional anggota ISO dan IEC berpartisipasi dalam pengembangan standardisasi internasional melalui panitia teknis yang disepakati oleh organisasi-organisasi yang terpercaya keahliannya dalam aktivitas-aktivitas teknis. Panitia Teknis ISO dan IEC berkolaborasi dengan prinsip saling menguntungkan. Organisasi-organisasi internasional lainnya, baik pemerintah maupun non-pemerintah, bekerja sama dengan ISO dan IEC, juga ambil bagian dalam kegiatan tersebut.

Di bidang teknologi informasi, ISO dan IEC telah menetapkan suatu Panitia Teknis Gabungan (ISO/IEC JTC 1). Rancangan standar internasional yang diadopsi oleh panitia teknis gabungan diedarkan kepada seluruh badan-badan nasional untuk diambil suara (voting). Penentuan sebagai satu sebuah standar internasional memerlukan persetujuan minimal 75% dari badan-badan nasional yang memberikan suara (pilihan).

Perlu diperhatikan terhadap kemungkinan bahwa beberapa elemen dari standar internasional ini, masih menjadi subyek bahasan hak-hak paten. Dalam hal ini, ISO dan IEC tidak bertanggung jawab untuk mengidentifikasi bagian manapun tentang hak-hak paten tersebut. Standar internasional ISO/IEC 17799 dipersiapkan oleh Institut Standar Inggris (dikenal sebagai BS 7799) dan diadopsi di bawah "prosedur jalur cepat" khusus oleh Panitia Teknis Gabungan ISO/IEC JTC 1, Teknologi Informasi, secara bersamaan dengan persetujuan dari badan-badan nasional ISO dan IEC).

Pentingya Keamanan Informasi

Informasi merupakan aset yang sangat berharga bagi sebuah organisasi karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha. Oleh karena itu maka perlindungan terhadap informasi (keamanan informasi) merupakan hal yang mutlak harus diperhatikan secara sungguh-sungguh oleh segenap jajaran pemilik, manajemen, dan karyawan organisasi yang bersangkutan. Keamanan informasi yang dimaksud menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman terhadapnya sehingga daapt menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup organisasi.

Informasi dikumpulkan, disimpan, diorganisasikan, dan disebarluaskan dalam berbagai bentuk - baik dokumen berbasis kertas hingga berkas elektronik. Apapun bentuk maupun cara penyimpanannya, harus selalu ada upaya dan untuk melindungi keamanannya sebaik mungkin. Keamanan yang dimaksud harus memperhatikan sejumlah aspek, yaitu:

1. Kerahasiaan - memastikan bahwa informasi tertentu hanya dapat diakses oleh mereka yang berhak atau memiliki wewenang untuk memperolehnya;
2. Integritas - melindungi akurasi dan kelengkapan informasi melalui sejumlah metodologi pengolahan yang efektif; dan
3. Ketersediaan - memastikan bahwa informasi terkait dapat diakses oleh mereka yang berwenang sesuai dengan kebutuhan.

Jaminan kemanan informasi dapat dicapai melalui aktivitas penerapan sejumlah kontrol yang sesuai. Kontrol yang dimaksud meliputi penerapan berbagai kebijakan, prosedur, struktur, praktek, dan fungsi-fungsi tertentu. Keseluruhan kontrol tersebut harus diterapkan oleh organisasi agar seluruh sasaran keamanan yang dimaksud dapat tercapai.

Alasan Keamanan Informasi

Menjaga keamanan informasi berarti pula perlunya usaha dalam memperhatikan faktor-faktor keamanan dari keseluruhan piranti pendukung, jaringan, dan fasilitas lain yang terkait langsung maupun tidak langsung dengan proses pengolahan informasi. Dengan amannya keseluruhan lingkungan tempat informasi tersebut berada, maka kerahasiaan, integritas, dan ketersediaan informasi akan dapat secara efektif berperan dalam meningkatkan keunggulan, keuntungan, nilai komersial, dan citra organisasi yang memiliki aset penting tersebut.

Adalah merupakan suatu kenyataan bahwa pada abad globalisasi ini, berbagai organisasi dihadapkan pada sejumlah ancaman-ancaman keamanan informasi dari berbagai sumber, seperti yang diperlihatkan dengan keberadaan sejumlah kasus kejahatan komputer secara sengaja, seperti: pencurian data, aktivitas spionase, percobaan *hacking*, tindakan vandalisme, dan lain-lain, maupun ancaman yang disebabkan karena kejadian-kejadian lain seperti bencana alam, misalnya: banjir, gempa bumi, tsunami, dan kebakaran. Bergantungnya kinerja organisasi pada sistem informasi mengandung arti bahwa keseluruhan ancaman terhadap keamanan tersebut merupakan portofolio resiko yang dihadapi oleh organisasi yang bersangkutan.

Perencanaan dan pengembangan sistem keamanan informasi yang baik semakin mendapatkan tantangan dengan adanya interkoneksi antara berbagai jaringan publik dan privat, terutama terkait dengan proses pemakaian bersama sejumlah sumber daya informasi untuk meningkatkan optimalisasi akses. Manfaat yang didapatkan melalui pendistribusian komputasi ini disaat yang sama melemahkan efektivitas kontrol secara terpusat, yang berarti pula menciptakan suatu kelemahan-kelemahan baru pada sistem tersebut. Kenyataan memperlihatkan bahwa sebagian besar sistem informasi yang dirancang dan dibangun dewasa ini kurang begitu memperhatikan faktor-faktor keamanan tersebut. Padahal untuk membangun sistem keamanan informasi yang baik, perlu dilakukan sejumlah langkah-langkah metodologis tertentu.

Keamanan informasi yang baik dapat dicapai melalui penerapan sejumlah upaya-upaya teknis (operasional) yang didukung oleh berbagai kebijakan dan prosedur manajemen yang sesuai. Proses tersebut dimulai dari pengidentifikasian sejumlah kontrol yang relevan untuk diterapkan dalam organisasi, yang tentu saja harus berdasarkan pada analisa kebutuhan aspek keamanan informasi seperti apa yang harus dimiliki perusahaan. Setelah kebijakan, prosedur, dan panduan teknis operasional mengenai kontrol-kontrol yang harus diterapkan dalam organisasi disusun, langkah berikutnya adalah sosialisasi keseluruhan piranti tersebut ke segenap lapisan manajemen dan karyawan organisasi untuk mendapatkan dukungan dan komitmen. Selanjutnya, para pihak berkepentingan lain yang berada di luar organisasi - seperti pemasok, pelanggan, mitra kerja, dan pemegang saham - harus pula dilibatkan dalam proses sosialisasi tersebut karena mereka merupakan bagian tidak terpisahkan dari sistem keamanan informasi yang dibangun. Keterlibatan sejumlah pakar maupun ahli dari luar organisasi kerap kali dibutuhkan untuk membantu organisasi dalam menerapkan langkah-langkah di tersebut. Dengan adanya pengetahuan yang mereka miliki, terutama dalam membantu organisasi menyusun kebutuhan dan mengidentifikasikan kontrol-kontrol yang dibutuhkan, niscaya sistem keamanan informasi yang dibangun dapat lebih efektif dan ekonomis.

Pemangku Kepentingan Keamanan Informasi

Dari penjabaran sebelumnya jelas terlihat bahwa semua pihak di dalam organisasi (manajemen dan karyawan) maupun di luar organisasi (pemasok, pelanggan, mitra kerja, dan pemegang saham) bertanggung jawab secara penuh dalam proses keamanan informasi. Hal tersebut disebabkan karena mereka semua terlibat secara langsung maupun tidak langsung dalam proses penyediaan, penyimpanan, pemanfaatan, dan penyebarluasan informasi dalam organisasi. Untuk menjamin adanya kesadaran, kemauan, dan komitmen untuk melakukan hal tersebut, maka perlu adanya pihak yang memiliki tugas dan kewajiban khusus untuk memantau efektivitas keamaman informasi tersebut. Keberadaan pihak tersebut mutlak dibutuhkan oleh organisasi dalam berbagai bentuknya, seperti: perusahaan komersial, institusi pemerintah, organisasi publik, lembaga nirlaba, dan lain sebagainya.

Strategi Sosialisasi Organisasi

Pemahaman dan kesadaran mengenai pentingnya memperhatikan aspek-aspek keamanan informasi harus ditanamkan sedini mungkin oleh setiap organisasi terhadap seluruh jajaran manajemen dan karyawannya. Setiap individu yang berada di dalam organisasi memiliki tanggung jawab untuk melindungi keamanan informasi yang dimilikinya, sebagaimana layaknya memperlakukan hal yang sama terhadap aset-aset berharga lainnya. Dalam kaitan dengan hal

ini, harus terdapat kebijakan menyangkut pemberian sanksi bagi mereka yang lalai memperhatikan hal ini maupun penghargaan bagi mereka yang berprestasi mempromosikan dan menerapkan keamanan informasi di organisasi terkait.

Implementasi Keamanan Informasi

Tentunya proses keamanan informasi harus dimulai dari menjaga tempat-tempat atau fasilitas fisik dimana informasi beserta piranti/peralatan pendukungnya disimpan. Mengingat bahwa hampir seluruh fungsi dalam organisasi memiliki tanggung jawab dalam mengelola informasinya masing-masing, maka setiap individu dalam berbagai fungsi-fungsi tersebut harus secara aktif menjaga keamanan informasi. Dengan berkembangnya teknologi akses informasi dari jarak jauh melalui pemanfaatan jaringan komputer, maka ruang lingkup keamanan menjadi semakin besar dan kompleks, karena sudah tidak dibatasi lagi oleh sekat-sekat lingkungan fisik tertentu. Perkembangan internet yang telah membentuk sebuah dunia maya tempat berbagai individu maupun komunitas berinteraksi (tukar menukar informasi) secara elektronik memperlihatkan bagaimana kompleksnya keamanan area baik secara fisik maupun virtual - yang tentu saja akan sangat berpengaruh terhadap manajemen kontrol yang akan dipilih dan diterapkan.

Cara Menerapkan Sistem Keamanan Informasi

Untuk dapat membangun dan menerapkan sistem keamanan informasi yang baik, sebaiknya organisasi memulainya dari upaya melakukan kajian atau telaah terhadap resiko-resiko keamanan yang mungkin timbul. Kajian yang dimaksud dapat diterapkan dalam tingkatan organisasi, maupun pada tataran sub bagian atau fungsi organisasi tertentu, seperti sistem informasi, komponen, layanan, dan lain sebagainya - sesuai dengan skala prioritas yang ada.Kajian resiko yang dimaksud merupakan suatu pendekatan sistematis dari proses:

1. Identifikasi terhadap kejadian-kejadian apa saja yang dapat mengancam keamanan informasi perusahaan dan potensi dampak kerugian yang ditimbulkan jika tidak terdapat kontrol yang memadai; dan
2. Analisa tingkat kemungkinan (probabilitas) terjadinya hal-hal yang tidak diinginkan tersebut akibat adanya sejumlah kelemahan pada sistem yang tidak dilindungi dengan kontrol tertentu.

Hasil dari kajian tersebut akan menghasilkan arahan yang jelas bagi manajemen dalam menentukan prioritas dan mengambil sejumlah tindakan terkait dengan resiko keamanan informasi yang dihadapi. Dengan adanya prioritas yang jelas maka akan dapat didefinisikan kontrol-kontrol mana saja yang perlu diterapkan. Perlu diperhatikan bahwa langkah-langkah tersebut harus dilakukan secara kontinyu dan periodik, mengingat dinamika perubahan organisasi dan lingkungan eksternal yang sedemikian cepat. Langkah-langkah interaktif yang dimaksud meliputi:

1. Menganalisa perubahan kebutuhan dan prioritas organisasi yang baru sesuai dengan pertumbuhannya;
2. Mempelajari ancaman-ancaman atau kelamahan-kelemahan baru apa yang terjadi akibat perubahan yang ada tersebut; dan
3. Memastikan bahwa kendali-kendali yang dimiliki tetap efektif dalam menghadapi ancaman-ancaman kejadian terkait.

Perlu dicatat bahwa peninjauan berkala tersebut harus dilakukan pada bagian organisasi dengan tingkat kedalaman tertentu sesuai dengan hasil analisa resiko yang telah dilakukan sebelumnya. Karena keberadaan kontrol ini akan sangat berpengaruh terhadap kinerja sebuah organisasi, maka proses telaah resiko harus dimulai dari tingkat, agar mereka yang berwenang dapat menilainya berdasarkan tingkat kepentingan terteinggi (pendekatan *top down*).

Standar dalam Keamanan Informasi

Keberadaan dan kepatuhan terhadap standar merupakan hal mutlak yang harus dimiliki oleh pihak manapun yang ingin menerapkan sistem keamanan informasi secara efektif. Sejumlah alasan utama mengapa standar diperlukan adalah untuk menjamin agar:

1. Seluruh pihak yang terlibat dalam proses keamanan informasi memiliki kesamaan pengertian, istilah, dan metodologi dalam melakukan upaya-upaya yang berkaitan dengan keamanan data;
2. Tidak terdapat aspek-aspek keamanan informasi yang terlupakan karena standar yang baik telah mencakup keseluruhan spektrum keamanan informasi yang disusun melalui pendekatan komprehensif dan holistik (utuh dan menyeluruh);

3. Upaya-upaya untuk membangun sistem keamanan informasi dilakukan secara efektif dan efisien dengan tingkat optimalisasi yang tinggi, karena telah memperhatikan faktor-faktor perkembangan teknologi serta situasi kondisi yang berpengaruh terhadap organisasi;
4. Tingkat keberhasilan dalam menghasilkan sistem keamanan informasi yang berkualitas menjadi tinggi, karena dipergunakan standar yang sudah teruji kehandalannya.

Penggunaan Dokumen Standar

Seperti yang telah dijelaskan sebelumnya, proses awal yang harus dilakukan setiap organisasi adalah melakukan kajian awal untuk mengidentifikasikan kebutuhan keamanan, mengingat setiap organisasi memiliki sifat uniknya masing-masing. Berdasarkan hasil tersebut, pilihlah kontrol-kontrol sesuai yang dapat diambil dalam dokumen standar ini, maupun dari sumber-sumber lain untuk melengkapinya manakala dibutuhkan. Setelah itu susunlah perencanaan program penerapan kontrol-kontrol yang dimaksud dengan melibatkan pihak internal maupun eksternal organisasi sesuai dengan kebutuhan. Perlu diperhatikan bahwa sejumlah kontrol sifatnya mutlak harus dimiliki oleh sebuah organisasi, sementara berbagai kontrol lainnya hakekatnya ditentukan oleh situasi dan kondisi organisasi yang bersangkutan. Disamping itu terdapat pula sejumlah kontrol yang harus diperhatikan secara sungguh-sungguh karena memiiki implikasi besar karena menyangkut kepentingan publik atau kontinuitas keberadaan organisasi.

Sepuluh Aspek Keamanan Informasi

Berikut adalah penjabaran ringkas dari sepuluh domain atau aspek yang harus diperhatikan terkait dengan isu keamanan informasi dalam sebuah organisasi atau institusi.

1. **Kebijakan Keamanan**: untuk memberikan arahan dan dukungan manajemen keamanan informasi. Manajemen harus menetapkan arah kebijakan yang jelas dan menunjukkan dukungan, serta komitmen terhadap keamanan informasi melalui penerapan dan pemeliharaan suatu kebijakan keamanan informasi di seluruh tataran organisasi;

2. **Pengorganisasian Keamanan**: untuk mengelola keamanan informasi dalam suatu organisasi. Satu kerangka kerja manajemen harus ditetapkan untuk memulai dan mengkontrol penerapan keamanan informasi di dalam organisasi.Fora manajemen

dengan kepemimpinan yang kondusif harus dibangun untuk menyetujui kebijakan keamanan informasi, menetapkan peran keamanan dan mengkoordinir penerapan keamanan di seluruh tataran organisasi. Jika diperlukan, pendapat pakar keamanan informasi harus dipersiapkan dan tersedia dalam organisasi. Hubungan dengan pakar keamanan eksternal harus dibangun untuk mengikuti perkembangan industri, memonitor standar dan metode penilaian serta menyediakan penghubung yang tepat, ketika berurusan dengan insiden keamanan. Pendekatan multi-disiplin terhadap keamanan informasi harus dikembangkan, misalnya dengan melibatkan kerjasama dan kolaborasi di antara manajer, pengguna, administrator, perancang aplikasi, pemeriksa dan staf keamanan, serta keahlian di bidang asuransi dan manajemen resiko;

3. **Klasifikasi dan Kontrol Aset**: untuk memelihara perlindungan yang tepat bagi pengorganisasian aset.Semua aset informasi penting harus diperhitungkan keberadaannya dan ditentukan kepemilikannya. Akuntabilitas terhadap aset akan menjamin terdapatnya perlindungan yang tepat. Pemilik semua aset penting harus diidentifikasi dan ditetapkan tanggung jawabnya untuk memelihara sistem kontrol tersebut. Tanggungjawab penerapan sistem kontrol dapat didelegasikan. Akuntabilitas harus tetap berada pada pemilik aset;

4. **Pengamanan Personil**: untuk mengurangi resiko kesalahan manusia, pencurian, penipuan atau penyalahgunaan fasilitas.Tanggung jawab keamanan harus diperhatikan pada tahap penerimaan pegawai, dicakup dalam kontrak dan dipantau selama masa kerja pegawai. Penelitian khusus harus dilakukan terhadap calon pegawai khususnya di bidang tugas yang rahasia. Seluruh pegawai dan pengguna pihak ketiga yang menggunakan fasilitas pemrosesan informasi harus menanda-tangani perjanjian kerahasiaan (non-disclosure);

5. **Keamanan Fisik dan Lingkungan**: untuk mencegah akses tanpa otorisasi, kerusakan, dan gangguan terhadap tempat dan informasi bisnis. Fasilitas pemrosesan informasi bisnis yang kritis dan sensitif harus berada di wilayah aman, terlindung dalam perimeter keamanan, dengan rintangan sistem pengamanan dan kontrol masuk yang memadai. Fasilitas tersebut harus dilindungi secara fisik dari akses tanpa ijin, kerusakan dan gangguan. Perlindungan harus disesuaikan dengan identifikasi resiko. Disarankan

penerapan kebijakan clear desk dan clear screen untuk mengurangi resiko akses tanpa ijin atau kerusakan terhadap kertas, media dan fasilitas pemrosesan informasi.

6. **Komunikasi dan Manajemen Operasi**: untuk menjamin bahwa fasilitas pemrosesan informasi berjalan dengan benar dan aman. Harus ditetapkan tanggungjawab dan prosedur untuk manajemen dan operasi seluruh fasilitas pemrosesan informasi. Hal ini mencakup pengembangan instruksi operasi yang tepat dan prosedur penanganan insiden. Dimana mungkin harus ditetapkan pemisahan tugas, untuk mengurangi resiko penyalahgunaan sistem karena kecerobohan atau kesengajaan;

7. **Pengontrolan Akses**: untuk mencegah akses tanpa ijin terhadap sistem informasi. Prosedur formal harus diberlakukan untuk mengkontrol alokasi akses, dari pendaftaran awal dari pengguna baru sampai pencabutan hak pengguna yang sudah tidak membutuhkan lagi akses ke sistem informasi dan layanan. Perhatian khusus harus diberikan, jika diperlukan, yang dibutuhkan untuk mengkontrol alokasi hak akses istimewa, yang memperbolehkan pengguna untuk menembus sistem kontrol;

8. **Pengembangan dan Pemeliharaan Sistem**: untuk memastikan bahwa keamanan dibangun dalam sistem informasi. Persyaratan Keamanan sistem mencakup infrastruktur, aplikasi bisnis dan aplikasi yang dikembangkan pengguna. Disain dan implementasi proses bisnis yang mendukung aplikasi atau layanan sangat menentukan bagi keamanan. Persyaratan keamanan harus diidentifikasi dan disetujui sebelum pengembangan sistem informasi. Semua persyaratan keamanan sisitem informasi, termasuk kebutuhan pengaturan darurat, harus diidentifikasi pada fase persyaratan suatu proyek., dan diputuskan, disetujui serta didokumentasikan sebagai bagian dari keseluruhan kasus bisnis sebuah sistem informasi;

9. **Manajemen Kelangsungan Bisnis**: Untuk menghadapi kemungkinan penghentian kegiatan usaha dan melindungi proses usaha yang kritis dari akibat kegagalan atau bencana besar. Proses manajemen kelangsungan usaha harus diterapkan untuk mengurangi kerusakan akibat bencana atau kegagalan sistem keamanan (yang mungkin dihasilkan dari, sebagai contoh, bencana alam, kecelakaan, kegagalan alat dan keterlambatan) sampai ke tingkat yang dapat ditolerir melalui kombinasi pencegahan

dan pemulihan kontrol. Konsekuensi dari bencana alam, kegagalan sistem keamanan dan kehilangan layanan harus dianalisa. Rencana darurat harus dikembangkan dan diterapkan untuk memastikan proses usaha dapat disimpan ulang dalam skala waktu yang dibutuhkan. Rencana semacam itu harus dijaga dan dipraktekkan untuk menjadi bagian integral keseluruhan proses manajemen. Manajemen kelangsungan bisnis harus mencakup kontrol untuk mengidentifikasi dan mengurangi resiko, membatasi konsekuensi kesalahan yang merusak, dan memastikan penyimpulan tahapan operasional yang penting; dan

10. **Kesesuaian**: Untuk menghindari pelanggaran terhadap hukum pidana maupun hukum perdata, perundangan, peraturan atau kewajiban kontrak serta ketentuan keamanan lainnya. Disain, operasional, penggunanan dan manajemenan sistem informasi adalah subyek dari perundangan, peraturan, dan perjanjian kebutuhan keamanan. Saran untuk kebutuhan legalitas yang bersifat khusus harus dicari dari penasihat hukum organisasi, atau praktisi hukum yang berkualitas. Kebutuhan legalitas bervariasi dari negara ke negara dan bagi informasi yang dihasilkan dalam satu negara yang didistribusikan ke negara lain (contohnya arus data lintas batas).