**Infrastruktur Manajemen Layananan Teknologi Informasi**

**Best Practise Keamanan SI/TI**

“**ISO 27001 *: untuk Sistem Manajemen Keamanan Informasi (SMKI)”.***

****

**Oleh :**

**Yulhendri**

**UNIVERSITAS ESA UNGGUL**

**FAKULTAS ILMU KOMPUTER**

**SISTEM INFORMASI**

**Pendahuluan**

**Latar Belakang**

**ISO 27001** adalah suatu standar internasional untuk Sistem Manajemen Keamanan Informasi (SMKI) sebagian besar sebelumnya diangkat berdasarkan BS 7799 yang umum digunakan sejak tahun 1995 mengenai pengelolaan keamanan informasi. ISO 27001 menyediakan kerangka kerja untuk netralitas penggunaan teknologi, netralitas sistem manajemen pengelolaan rekanan yang memungkinkan suatu organisasi memastikan bahwa efektif dalam pengukuran keamanan informasi. Hal ini termasuk kemampuan mengakses data secara berkelanjutan, adanya kerahasiaan dan integritas atas informasi yang dimilikinya dan kebutuhan pihak-pihak yang berkepentingan demikian pula dengan kesesuaian hokum.

Sedangkan *Information Security Management System* (ISMS) adalah suatu cara untuk melindungi dan mengelola informasi berdasarkan pendekatan yang sistematis terhadap resiko bisnis, untuk mempersiapkan, mengimplementasikan, mengoperasikan, mengawasi, meninjau kembali, memelihara, serta meningkatkan pengamanan informasi.

ISO 27001 disusun agar mudah saling melengkapi dengan standar sistem manajemen lainnya seperti ISO 9001 dan ISO 14001. Meskipun komunikasi moderen memerlukan suatu perantara berarti bahwa sebagian terbesar sistem ISMS diutamakan pada ICT, ISO 27001 adalah penerapan yang seimbang pada bentuk-bentuk informasi, seperti catatan, gambar, dan percakapan yang tersaji dalam bentuk kertas.

**Rumusan Masalah**

**Manfaat**

* ISO 27001 memastikan adanya keamanan dalam sistem mutu yang digunakan saat ini,
* ISO 27001 memberikan kesempatan untuk mengidentifikasi dan mengelola resiko informasi dan sistem,
* Memberikan kepercayaan diri dan jaminan kepada organisasi mitra dagang dan klien,
* Memungkinkan audit independen dalam praktek-praktek keamanan informasi.

**Pembahasan**

Kejadian berikut ini merupakan kejadian nyata yang terjadi di sebuah perusahaan besar di Indonesia. Namun, beberapa aspek dari kejadian ini harus penulis samarkan dengan beberapa alasan. Pada awal tahun 2006, PT “A” geger, dikarenakan pada suatu pagi di hari Senin, ketika semua karyawan mulai kembali beraktivitas setelah libur panjang, sebuah e-mail masuk ke seluruh *mailbox* karyawan dengan sebuah *attachment* berupa file excel yang di dalamnya berisi data dan informasi gaji ribuan karyawan di perusahaan tersebut.

Coba bayangkan efek dari kejadian ini, ketika tiba-tiba seorang karyawan menjadi tahu gaji rekannya yang kebetulan memiliki tingkat pekerjaan yang sama, namun bergaji jauh lebih tinggi. Begitu pula seorang staf yang tiba-tiba mengetahui gaji atasannya.

Investigasi dengan serta-merta pun dilakukan oleh pihak teknologi informasi perusahaan tersebut dengan dipimpin langsung oleh vice president IT. Karena file excel tersebut dikirim melalui e-mail, maka pasti ada pengirimnya, sebut saja Bapak ‘B’. Namun penyelidikan kemudian menemukan jalan buntu, karena pada hari serta tanggal pengiriman yang tertera pada e-mail, Bapak ‘B’ ini sedang bertugas di salah satu lokasi kantor cabang yang tidak memiliki koneksi Internet, dan ada banyak saksi yang bersedia memberikan keterangan bahwa beliau sama sekali tidak dapat mengakses sistem e-mail perusahaan selama sehari penuh bahkan hingga beberapa ke depan.

Investigasi secara teknis pun dilakukan dengan memeriksa *access log,* baik pada sistem e-mail maupun LDAP untuk melihat siapa saja staf atau karyawan di perusahaan tersebut yang melakukan akses pada hari dan jam terkirimnya e-mail tersebut. Namun celakanya, seseorang dengan cerdiknya telah berhasil menghapus “jejak”, sehingga tim penyelidik kembali mendapatkan hasil nol besar. Kesimpulan sementara dari hasil penyelidikan akhirnya hanya mengindikasikan bahwa Bapak “B” telah dijebak, dan seseorang dengan tingkat pengetahuan serta *skill* teknis yang cukup tinggi, telah mengakses data dan informasi gaji tersebut dari pihak *payroll*, mengirimnya dengan menggunakan e-mail account Bapak ‘B’, lalu dengan cerdik menghapus semua jejaknya. Tanpa tahu siapa yang sebenarnya telah melakukan tindakan ini serta apa motifnya.

Tim investigasi internal juga melakukan beberapa perubahan konfigurasi pada sistem e-mail perusahaan serta memperketat aktivitas pengawasan secara digital yang antara lain adalah memusatkan penyimpanan log-log aktivitas setiap system di dalam *data center*. Hal ini diharapkan akan dapat menghindari kejadian-kejadian yang sama di masa depan. Selesai sampai di sini? Ternyata tidak. Tepat satu bulan kemudian, e-mail heboh tersebut kembali terkirim ke seluruh mailbox karyawan PT “A”, masih dengan isi yang sama dan pengirim yang sama, dan kembali terulang lagi untuk ketiga kalinya di bulan berikutnya.

Kejadian tersebut juga memberikan gambaran kepada kita bahwa sekuat apapun kita memasang perangkat keamanan di infrastruktur teknologi informasi di kantor, katakanlah sistem *firewall* tiga lapis dengan merek yang berbeda-beda, antivirus yang juga diimplementasikan secara komplementer dari dua merk berbeda serta keamanan fisik lainnya seperti implementasi perangkat biometric di data center. Masih belum cukup untuk “mengusir” tangan-tangan jahil orang-orang yang tidak bertanggung jawab.

PT “A” seperti contoh di atas, bukanlah sebuah perusahaan yang “pemula” di bidang teknologi informasi. Investasi teknologi informasi perusahaan ini pernah pada suatu tahun fiskal tertentu nyaris mendekati angka Rp 1 milyar. Pembangunan sistem serta teknologi informasinya juga dipandu langsung oleh sebuah perusahaan integrasi sistem terbesar di dunia. Namun ternyata semua itu masih belum cukup, karena sebuah data yang sifatnya rahasia ternyata masih juga dapat tersebar hingga menyebabkan terjadinya perubahan suasana kerja yang cukup signifikan terhadap produktivitas perusahaan.

Dampak psikologis, baik secara organisasi maupun perorangan dari kejadian ini ternyata cukup masif kuantitas dan kualitasnya. Akhirnya beberapa perubahan serta tindakan pencegahan yang cukup agresif dilakukan oleh pihak manajemen dengan tujuan agar kejadian tersebut tidak lagi terulang di masa depan.

Information Security Management System (ISMS) merupakan sebuah kesatuan sistem yang disusun berdasarkan pendekatan resiko bisnis untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan.

Sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut yang menjadi objek yang akan diteliti, antara lain:

* **Struktur organisasi**
* **Kebijakan keamanan (security policy)**
* **Prosedur dan proses**
* **Tanggung jawab atau responsibility** ™ **Sumber Daya Manusia**

Masalah yang ingin diteliti pada objek penelitian ini, adalah

**Struktur organisasi pengelola jaringan dan keamanan informasi**. ”apakah struktur organisasi yang ada saat ini sudah mengakomodir kebutuhan akan orang atau departemen yang bertanggung jawab secara khusus untuk membangun jaringan komputer dan sistem informasi yang secara terus menerus dimonitoring, dikembangkan, dijaga keamanan dan ketersediaannya?

**Tindakan preventif dan kepedulian pengguna jaringan yang memanfaatkan informasi.** Apakah semua permasalahan jaringan dan kejadian pelanggaran keamanan atas setiap kelemahan sistem informasi telah ”segera” dilaporkan sehingga administrator (jaringan maupun database perusahaan) akan segera mengambil langkah-langkah keamanan yang dianggap perlu.

Apakah **akses terhadap sumber daya pada jaringan** sudah dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak.

Apakah **akses terhadap sistem komputasi dan informasi serta periferalnya** juga koneksi ke jaringan telah diatur dengan baik, termasuk logon pengguna.

Apakah **pengelolaan account** sudah dikelola secara benar untuk menjamin bahwa hanya orang/peralatan yang diotorisasi yang dapat terkoneksi ke jaringan?

**A**pakah semua **prosedur serta proses-proses yang terkait dengan usaha-usaha pengimplementasian keamanan informasi** di perusahaan sudah dijalankan dengan benar?” Misalnya prosedur permohonan ijin akses aplikasi, akses *hotspot*, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya.

Sudahkah perusahaan melaksanakan ketentuan dimaksud dan memberikan **pelatihan dan sosialisasi** yang cukup bagi **setiap individu** untuk **sadar** **akan pentingnya upaya menjaga keamanan informasi**?

**Policy dan tindakan yang ditetapkan** perusahaan dalam melindungi sistem keamanan jaringan dan informasi apakah sudah dilaksanakan dengan benar?.

**Tujuan Implementasi ISO 27001**

Implementasi ISO/IEC 27001:2005 ini bertujuan untuk memberikan gambaran implementasi sistem manajemen keamanan informasi berstandar internasional kepada perusahaan, organisasi nirlaba, instansi atau publik agar dapat mempelajari dan mencoba mengimplementasikannya dilingkungan sendiri.

Implementasi ISO/IEC 27001:2005 pada kegiatannya juga mencoba melakukan kegiatan audit terhadap semua aspek terkait, seperti: kondisi jaringan komputer lokal, policy, manajemen SDM, organisasi keamanan informasi, dan lain-lain.

**Tujuan Audit dan Manfaat Penetapan ISO/IEC 27001:2005**

* Audit ISMS memberi pemahaman yang lebih baik mengenai aset informasi dan proses manajemen keamanan informasi yang diperlukan.
* Membantu memberikan pemahaman pentingnya keamanan informasi pada karyawan, stakeholder dan masyarakat umum,
* Membantu mengarahkan implementasi sistem manajemen keamanan informasi berdasarkan kepada pertimbangan manajemen risiko.
* Mendukung organisasi dengan memberi kerangka kerja (panduan) proses untuk mengimplementasikan dan melakukan manajemen serta kontrol terhadap keamanan informasi agar dapat menjamin bahwa objek-objek keamanan tertentu telah dicapai.
* Membantu organisasi untuk menjaminkan risiko keamanan dapat dikendalikan dengan biaya terkontrol dan dengan feedback yang menguntungkan,
* Meningkatkan keyakinan terhadap organisasi karena telah mematuhi undang-undang, peraturan-peraturan negara, dengan menjamin kualitas informasi dan pelayanan.
* Mempersilakan auditor internal maupun external untuk memastikan bahwa organisasi telah mematuhi aturan-aturan, memiliki arah pengembangan Manajemen dan standard-standard yang dilaksanakan.

Simbol untuk kualitas dan keamanan. Penetapan ISO/IEC 27001:2005 akan menunjukkan kepada pelanggan-pelanggan, partner anda dan pihak pemerintah bahwa kualitas pelayanan dan keamanan yang baik dalam proses bisnis anda telah dikendalikan dengan benar, hal ini dapat menjadi publikasi yang sangat positif bagi organisasi untuk meraih kepercayaan stake holder.

**Tinjauan Pustaka dan Landasan Teori**

**Keamanan Informasi**

 Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. Kebanyakan orang mungkin akan bertanya, mengapa “keamanan informasi” dan bukan “keamanan teknologi informasi” atau IT Security. Kedua istilah ini sebenarnya sangat terkait, namun mengacu pada dua hal yang sama sekali berbeda. “Keamanan Teknologi Informasi” atau IT Security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan.

 Berbeda dengan “keamanan informasi” yang fokusnya justru pada data dan informasi milik perusahaan Pada konsep ini, usahausaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan.

 Berdasarkan penjelasan tersebut, ‘kemananan teknologi informasi’ merupakan bagian dari keseluruhan aspek ‘keamanan informasi’. Karena teknologi informasi merupakan salah satu alat atau tool penting yang digunakan untuk mengamankan akses serta penggunaan dari data dan informasi perusahaan. Dari pemahaman ini pula, kita akan mengetahui bahwa teknologi informasi bukanlah satusatunya aspek yang memungkinkan terwujudnya konsep keamanan informasi di perusahaan.

 Keamanan informasi terdiri dari perlindungan terhadap aspekaspek berikut:

*Confidentiality (kerahasiaan)* aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

*Integrity (integritas)* aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.

*Availability (ketersediaan)* aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

 Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakankebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.



**Gambar 1 Elemen-elemen Keamanan Informasi**

Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar.

Hasil survey ISBS (Information Security Breaches Survey) pada tahun 2000 menunjukkan bahwa sebagian besar data atau informasi tidak cukup terpelihara/terlindungi sehingga beralasan kerawanan. Hasil survey yang terkait dengan hal ini dapat dilihat dalam gambar berikut:



**Gambar 2 Grafik Persentase Ancaman Keamanan Sistem**

**Informasi**

Survey tersebut juga menunjukkan bahwa 60% organisasi mengalami serangan atau kerusakan data karena kelemahan dalam sistem keamanan. Kegagalan sistem keamanan lebih banyak disebabkan oleh faktor internal dibandingkan dengan faktor eksternal. Faktor internal ini diantaranya kesalahan dalam pengoperasian sistem (40%) dan diskontinuitas power supply (32%).

Hasil survey ISBS tahun 2004-2006 menunjukkan bahwa terdapat banyak jaringan bisnis di Inggris (UK) telah mendapatkan serangan dari luar.



**Gambar 3 UK Business Network Attack**

Langkah-langkah untuk memastikan bahwa sistem benar-benar mampu menjamin keamanan data dan informasi dapat dilakukan dengan menerapkan kunci-kunci pengendalian yang teridentifikasi dalam standar ini.

**Dasar Manajemen Keamanan Informasi** **Informasi Sebagai Aset**

 Informasi adalah salah satu aset bagi sebuah perusahaan atau organisasi, yang sebagaimana aset lainnya memiliki nilai tertentu bagi perusahaan atau organisasi tersebut sehingga harus dilindungi, untuk menjamin kelangsungan perusahaan atau organisasi, meminimalisir kerusakan karena kebocoran sistem keamanan informasi, mempercepat kembalinya investasi dan memperluas peluang usaha [1]. Beragam bentuk informasi yang mungkin dimiliki oleh sebuah perusahaan atau organisasi meliputi diantaranya: informasi yang tersimpan dalam komputer (baik *desktop* komputer maupun *mobile* komputer), informasi yang ditransmisikan melalui network, informasi yang dicetak pada kertas, dikirim melalui fax, tersimpan dalam disket, CD, DVD, flashdisk, atau media penyimpanan lain, informasi yang dilakukan dalam pembicaraan (termasuk percakapan melalui telepon), dikirim melalui telex, email, informasi yang tersimpan dalam database, tersimpan dalam film, dipresentasikan dengan OHP atau media presentasi yang lain, dan metode-metode lain yang dapat digunakan untuk menyampaikan informasi dan ide-ide baru organisasi atau perusahaan [2].

**Informasi perlu dilindungi keamanannya** Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan, secara umum diartikan sebagai “*quality or state of being secure-to be free from danger”*  [1]. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan yang lainnya. Strategi keamanan informasi memiliki fokus dan dibangun pada masingmasing ke-khusus-annya. Contoh dari tinjauan keamanan informasi adalah:

*Physical Security* yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.

*Personal Security* yang overlap dengan ‘*phisycal security’* dalam melindungi orang-orang dalam organisasi.

*Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.

*Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.

*Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

 Masing-masing komponen di atas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan, menyimpan, dan mengirimkannya . Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha .

**Persyaratan umum**

Organisasi harus menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan ISMS yang terdokumentasi dalam konteks keseluruhan kegiatan bisnis organisasi dan risiko yang dihadapinya. Untuk keperluan Standar Internasional ini proses yang digunakan didasarkan pada model PDCA yang ditunjukkan pada Gambar 1.

**Menetapkan ISMS**

Organisasi harus melakukan hal berikut.

* Menentukan ruang lingkup dan batas-batas SMKI dalam hal karakteristik bisnis, organisasi, lokasi, aset, dan teknologi, dan termasuk perincian dan pembenaran untuk pengecualian dari ruang lingkup (lihat 1.2).
* Menentukan kebijakan SMKI dalam hal karakteristik bisnis, organisasi, lokasi, aset, dan teknologi yang:
* termasuk kerangka kerja untuk menetapkan tujuan dan membangun rasa arah dan prinsip-prinsip untuk tindakan terkait keamanan informasi;
* memperhitungkan persyaratan bisnis dan hukum atau peraturan, dan kewajiban keamanan kontraktual;
* sejalan dengan konteks manajemen risiko strategis organisasi di mana pembentukan dan pemeliharaan SMKI akan berlangsung;
* menetapkan kriteria yang akan dievaluasi risiko (lihat 4.2.1c)); dan
* telah disetujui oleh manajemen.
* Menentukan pendekatan penilaian risiko organisasi.
* Identifikasi metodologi penilaian risiko yang sesuai dengan SMKI, dan keamanan informasi bisnis yang teridentifikasi, persyaratan hukum dan peraturan.
* Mengembangkan kriteria untuk menerima risiko dan mengidentifikasi tingkat risiko yang dapat diterima. (lihat 5.1f)).

Metodologi penilaian risiko yang dipilih harus memastikan bahwa penilaian risiko menghasilkan hasil yang sebanding dan dapat direproduksi.

* Identifikasi risiko.
* Identifikasi aset dalam ruang lingkup ISMS, dan pemilik aset ini.
* Identifikasi ancaman terhadap aset tersebut.
* Identifikasi kerentanan yang mungkin dieksploitasi oleh ancaman.
* Identifikasi dampak hilangnya kerahasiaan, integritas, dan ketersediaan pada aset.
* Menganalisis dan mengevaluasi risiko.
* Menilai dampak bisnis terhadap organisasi yang mungkin timbul dari kegagalan keamanan, dengan mempertimbangkan konsekuensi dari hilangnya kerahasiaan, integritas, atau ketersediaan aset.
* Menilai kemungkinan realistis kegagalan keamanan yang terjadi sehubungan dengan ancaman dan kerentanan yang ada, dan dampak yang terkait dengan aset ini, dan kontrol yang saat ini diterapkan.
* Perkirakan tingkat risiko.
* Menentukan apakah risiko dapat diterima atau memerlukan perawatan menggunakan kriteria untuk menerima risiko yang ditetapkan dalam 4.2.1c)
* Mengidentifikasi dan mengevaluasi opsi untuk perawatan risiko.

Tindakan yang mungkin dilakukan meliputi:

* menerapkan kontrol yang sesuai;
* menerima risiko secara sadar dan obyektif, asalkan mereka jelas memenuhi kebijakan organisasi dan kriteria untuk menerima risiko (lihat 4.2.1c) 2));
* menghindari risiko; dan
* mentransfer risiko bisnis terkait ke pihak lain, mis. perusahaan asuransi, pemasok.
* Pilih tujuan dan kontrol kontrol untuk perawatan risiko.

Tujuan dan kontrol pengendalian harus dipilih dan diimplementasikan untuk memenuhi persyaratan yang diidentifikasi oleh penilaian risiko dan proses perlakuan risiko. Seleksi ini harus mempertimbangkan kriteria untuk menerima risiko (lihat 4.2.1c) 2)) serta persyaratan hukum, peraturan, dan kontrak.

Tujuan kontrol dan kontrol dari Lampiran A harus dipilih sebagai bagian dari proses ini yang sesuai untuk mencakup persyaratan yang diidentifikasi.

Tujuan kontrol dan kontrol yang tercantum dalam Lampiran A tidak lengkap dan tujuan kontrol dan kontrol tambahan juga dapat dipilih.

* Dapatkan persetujuan manajemen dari risiko residual yang diusulkan.
* Dapatkan otorisasi manajemen untuk menerapkan dan mengoperasikan ISMS.
* Menyiapkan Pernyataan Keberlakuan.
* Pernyataan Keberlakuan harus disiapkan yang meliputi:
* tujuan kontrol dan kontrol yang dipilih dalam 4.2.1g) dan alasan pemilihannya;
* tujuan kontrol dan kontrol yang saat ini diterapkan (lihat 4.2.1e) 2)); dan
* pengecualian tujuan kontrol dan kontrol dalam Lampiran A dan pembenaran untuk pengecualian mereka.

**Memantau dan meninjau ISMS**

Organisasi harus melakukan hal berikut.

* Jalankan pemantauan dan meninjau prosedur dan kontrol lainnya untuk:
* segera mendeteksi kesalahan dalam hasil pemrosesan;
* segera mengidentifikasi pelanggaran dan insiden keamanan yang dicoba dan berhasil;
* memungkinkan manajemen untuk menentukan apakah kegiatan keamanan yang didelegasikan kepada orang-orang atau dilaksanakan oleh teknologi informasi melakukan seperti yang diharapkan;
* membantu mendeteksi peristiwa keamanan dan dengan demikian mencegah insiden keamanan dengan menggunakan indikator; dan
* menentukan apakah tindakan yang diambil untuk menyelesaikan pelanggaran keamanan efektif
* Melakukan tinjauan berkala terhadap efektivitas ISMS (termasuk memenuhi kebijakan dan tujuan ISMS, dan meninjau kontrol keamanan) dengan mempertimbangkan hasil audit keamanan, insiden, hasil dari pengukuran efektivitas, saran dan umpan balik dari semua pihak yang berkepentingan.
* Mengukur efektivitas kontrol untuk memverifikasi bahwa persyaratan keamanan telah dipenuhi.
* Tinjau penilaian risiko pada interval yang direncanakan dan tinjau risiko residual dan tingkat risiko yang dapat diterima yang diidentifikasi, dengan mempertimbangkan perubahan pada:
* organisasi;
* teknologi;
* tujuan dan proses bisnis;
* ancaman yang teridentifikasi;
* efektivitas kontrol yang diterapkan; dan
* peristiwa eksternal, seperti perubahan lingkungan hukum atau peraturan, perubahan kewajiban kontrak, dan perubahan iklim sosial.
* Melakukan audit ISMS internal pada interval yang direncanakan (lihat 6).
* Melakukan tinjauan manajemen terhadap SMKI secara teratur untuk memastikan bahwa ruang lingkupnya tetap memadai dan perbaikan dalam proses SMKI diidentifikasi (lihat 7.1).
* Memperbarui rencana keamanan untuk memperhitungkan temuan kegiatan pemantauan dan peninjauan.
* Catat tindakan dan peristiwa yang dapat berdampak pada efektivitas atau kinerja SMKI (lihat 4.3.3).

 **Memelihara dan meningkatkan ISMS**

Organisasi harus secara teratur melakukan hal berikut.

* Menerapkan perbaikan yang diidentifikasi dalam SMKI.
* Mengambil tindakan korektif dan preventif yang sesuai sesuai dengan 8.2 dan 8.3. Terapkan pelajaran yang dipetik dari pengalaman keamanan organisasi lain dan dari organisasi itu sendiri.
* Komunikasikan tindakan dan perbaikan kepada semua pihak yang berkepentingan dengan tingkat perincian yang sesuai dengan keadaan dan, jika relevan, sepakati cara melanjutkan.
* Pastikan bahwa perbaikan mencapai tujuan yang dimaksudkan.

**Aspek Lain Keamanan Informasi**

Keamanan informasi memiliki beberapa aspek yang harus dipahami untuk dapat diterapkan. Beberapa aspek tersebut, tiga yang pertama disebut C.I.A (*Confidentiality, Integrity & Availability) ”triangle model”* [Gambar 3.1 Elemen-elemen keamanan informasi], seperti yang diuraikan pada point 3.1 Keamanan Informasi (pembahasan sebelumnya).

 Aspek yang lain disebutkan oleh Dr. Michael E.Whitman dan Herbert J. Mattord dalam bukunya Management Of Information Security adalah:

*Privacy*

Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik.

*Identification*

Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali individu pengguna. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi secara umum dilakukan dalam penggunaan *user name* atau *user ID.*

*Authentication*

Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang mereka klaim.

*Authorization*

Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia ataupun komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari aset informasi.

*Accountability*

Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktifitas terhadap aset informasi yang telah dilakukan, dan siapa yang melakukan aktifitas itu.

**Manajemen**

Sangat penting memahami beberapa prinsip dalam manajemen. Secara sederhana, manajemen adalah proses untuk mencapai tujuan dengan menggunakan sumberdaya yang ada [3]. Manajer adalah seseorang yang bekerja dengan orang lain dan melalui orang lain dengan cara mengkoordinasi kerja mereka untuk memenuhi tujuan organisasi. Tugas manajer adalah untuk memimpin pengelolaan sumberdaya organisasi, melakukan koordinasi penyelesaian pekerjaan orang-orang dalam organisasi, dan memegang aturan-aturan yang diperlukan untuk memenuhi tujuan organisasi. Diantara aturan-aturan itu adalah:

*Aturan informasi*: mengumpulkan, memproses, dan menggunakan informasi yang dapat mempengaruhi pencapaian tujuan.

*Aturan interpersonal*: berinteraksi dengan *stakeholder* dan orang atau organisasi lain yang mempengaruhi atau dipengaruhi oleh tercapainya tujuan organisasi dimana dia menjadi manajer.

*Aturan keputusan*: memilih diantara beberapa alternatif pendekatan, memecahkan konflik, dilema atau tantangan.

Manajer mengelola sumberdaya organisasi meliputi perencanaan biaya organisasi, otorisasi pengeluaran biaya, dan menyewa pekerja.

**Manajemen Keamanan Informasi**

Sebagaimana telah disebutkan sebelumnya bahwa manajemen keamanan informasi adalah satu dari tiga bagian dalam komponen keamanan informasi menurut NSTISSC. Sebagai bagian dari keseluruhan manajemen, tujuan manajemen keamanan informasi berbeda dengan manajemen teknologi informasi dan manajemen umum, karena memfokuskan diri pada keamanan operasi organisasi. Manajemen keamanan informasi memiliki tanggung jawab untuk program khusus, maka ada karakteristik khusus yang harus dimilikinya, yang dalam manajemen keamanan informasi dikenal sebagai 6P yaitu:

**Planning**

*Planning* dalam manajemen keamanan informasi meliputi proses perancangan, pembuatan, dan implementasi strategi untuk mencapai tujuan. Ada tiga tahapannya yaitu:

*strategic planning* yang dilakukan oleh tingkatan tertinggi dalam organisasi untuk periode yang lama, biasanya lima tahunan atau lebih,

*tactical planning* memfokuskan diri pada pembuatan perencanaan dan mengintegrasi sumberdaya organisasi pada tingkat yang lebih rendah dalam periode yang lebih singkat, misalnya satu atau dua tahunan,

*operational planning* memfokuskan diri pada kinerja harian organisasi. Sebagi tambahannya, planning dalam manajemen keamanan informasi adalah aktifitas yang dibutuhkan untuk mendukung perancangan, pembuatan, dan implementasi strategi keamanan informasi supaya diterapkan dalam lingkungan teknologi informasi. Ada beberapa tipe planning dalam manajemen keamanan informasi, meliputi : ™ *Incident Response Planning (IRP)*

IRP terdiri dari satu set proses dan prosedur detil yang mengantisipasi, mendeteksi, dan mengurangi akibat dari insiden yang tidak diinginkan yang membahayakan sumberdaya informasi dan aset organisasi, ketika insiden ini terdeteksi benar-benar terjadi dan mempengaruhi atau merusak aset informasi. Insiden merupakan ancaman yang telah terjadi dan menyerang aset informasi, dan mengancam *confidentiality*, *integrity* atau *availbility* sumberdaya informasi. *Insident Response Planning* meliputi *incident detection*, *incident response*, dan *incident recovery*.

™ *Disaster Recovery Planning* (DRP)

*Disaster Recovery Planning* merupakan persiapan jika terjadi bencana, dan melakukan pemulihan dari bencana. Pada beberapa kasus, insiden yang dideteksi dalam IRP dapat dikategorikan sebagai bencana jika skalanya sangat besar dan IRP tidak dapat lagi menanganinya secara efektif dan efisien untuk melakukan pemulihan dari insiden itu. Insiden dapat kemudian dikategorikan sebagai bencana jika organisasi tidak mampu mengendalikan akibat dari insiden yang terjadi, dan tingkat kerusakan yang ditimbulkan sangat besar sehingga memerlukan waktu yang lama untuk melakukan pemulihan. ™ *Business Continuity Planning* (BCP)

Business Continuity Planning menjamin bahwa fungsi kritis organisasi tetap bisa berjalan jika terjadi bencana. Identifikasi fungsi kritis organisasi dan sumberdaya pendukungnya merupakan tugas utama business continuity planning. Jika terjadi bencana, BCP bertugas menjamin kelangsungan fungsi kritis di tempat alternatif. Faktor penting yang diperhitungkan dalam BCP adalah biaya.

**Policy**

Dalam keamanan informasi, ada tiga kategori umum dari kebijakan yaitu:

*Enterprise Information Security Policy (EISP)* menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.

*Issue Spesific Security Policy (ISSP)* adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi keamanan informasi pada setiap teknologi yang digunakan, misalnya e-mail atau penggunaan internet.

*System Spesific Policy (SSP)* pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

**Programs**

Adalah operasi-operasi dalam keamanan informasi yang secara khusus diatur dalam beberapa bagian. Salah satu contohnya adalah program security education training and awareness. Program ini bertujuan untuk memberikan pengetahuan kepada pekerja mengenai keamanan informasi dan meningkatkan pemahaman keamanan informasi pekerja sehingga dicapai peningkatan keamanan informasi organisasi.

**Protection**

Fungsi proteksi dilaksanakan melalui serangkaian aktifitas manajemen resiko, meliputi perkiraan resiko (*risk assessment*) dan pengendali, termasuk mekanisme proteksi, teknologi proteksi dan perangkat proteksi baik perangkat keras maupun perangkat keras. Setiap mekanisme merupakan aplikasi dari aspek-aspek dalam rencana keamanan informasi.

**People**

Manusia adalah penghubung utama dalam program keamanan informasi. Penting sekali mengenali aturan krusial yang dilakukan oleh pekerja dalam program keamanan informasi. Aspek ini meliputi personil keamanan dan keamanan personil dalam organisasi.

**Project Management**

 Komponen terakhir adalah penerapan kedisiplinan manajemen dalam setiap elemen kemanan informasi. Hal ini melibatkan identifikasi dan pengendalian sumberdaya yang dikerahkan untuk keamanan informasi, misalnya pengukuran pencapaian keamanan informasi dan peningkatannya dalam mencapai tujuan keamanan informasi.

**Perlunya Manajemen Keamanan Informasi**

Manajemen keamanan informasi diperlukan karena ancaman terhadap C.I.A (*triangle model*) aset informasi semakin lama semakin meningkat. Menurut survey UK Department of Trade and Industry pada tahun 2000, 49% organisasi meyakini bahwa informasi adalah aset yang penting karena kebocoran informasi dapat dimanfaatkan oleh pesaing, dan 49% organisasi meyakini bahwa keamanan informasi sangat penting untuk memperoleh kepercayaan konsumen. Organisasi menghadapi berbagai ancaman terhadap informasi yang dimilikinya, sehingga diperlukan langkah-langkah yang tepat untuk mengamankan aset informasi yang dimiliki.

**Standarisasi Sistem Manajemen Keamanan Informasi**

Ada banyak sekali model manajemen keamanan informasi dan penerapannya, karena banyaknya konsultan keamanan informasi yang menawarkannya, masing-masing memfokuskan diri pada area yang berbeda dalam praktek manajemen keamanan informasi.

BS 7799:1, sekarang dikenal sebagai ISO/IEC 17799 setelah diadopsi oleh ISO, disebut sebagai Information Technology Code of Practice for Information Security Management.

BS 7799:2 disebut sebagai Information Security Management: Specification with Guidance for Use.

ISO/IEC 27001 adalah standar information security yang diterbitkan pada Oktober 2005 oleh International Organization for Standarization (ISO) dan International Electrotechnical Commission (IEC). Standar ini menggantikan BS-77992:2002 (British Standard).

General Accepted System Security Principles atau “GASSP”, yang merupakan bagian dari kumpulan penerapan sistem keamanan informasi.

Guidelines for the Management of IT Security, atau GMITS / ISO-13335, yang menyediakan sebuah konsep kerangka kerja (framework) untuk manajemen keamanan IT.

Mendapatkan dokumen Standar ISO ini, organisasi/perusahaan/istansi yang akan menerapkannya harus membayarnya dan biasanya meminta bimbingan fihak konsultan yang memahami proses sertifikasi ISO tersebut.

**ISO/IEC 27001: 2005**

ISO/IEC 27001 adalah standar information security yang diterbitkan pada October 2005 oleh International Organization for Standarization dan International Electrotechnical Commission. Standar ini menggantikan BS-77992:2002.

ISO/IEC 27001: 2005 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO/IEC 27001: 2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa dan memelihara seta mendokumentasikan Information Security Management System dalam konteks resiko bisnis organisasi keseluruhan

ISO/IEC 27001 mendefenisikan keperluan-keperluan untuk sistem manajemen keamanan informasi (ISMS). ISMS yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari resiko kerugian/bencana dan kegagalan serius pada pengamanan sistem informasi, implementasi ISMS ini akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang tidak lama.

**Information Security Management System**

Information Security Management System (ISMS) merupakan sebuah kesatuan system yang disusun berdasarkan pendekatan resiko bisnis, untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan. Dan sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut:

**Struktur organisasi**, biasarnya berupa keberadaan fungsi-fungsi atau jabatan organisasi yang terkait dengan keamanan informasi. Misalnya; Chief Security Offi cer dan beberapa lainnya.

**Kebijakan keamanan,** atau dalam bahasa Inggris disebut sebagai *Security Policy*. Contoh kebijakan keamanan ini misalnya adalah sebagai berikut: Semua kejadian pelanggaran keamanan dan setiap kelemahan sistem informasi harus segera dilaporkan dan administrator harus segera mengambil langkah-langkah keamanan yang dianggap perlu. Akses terhadap sumber daya pada jaringan harus dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak. Akses terhadap sistem komputasi dan informasi serta periferalnya harus dibatasi dan koneksi ke jaringan, termasuk logon pengguna, harus dikelola secara benar untuk menjamin bahwa hanya orang/ peralatan yang diotorisasi yang dapat terkoneksi ke jaringan.

**Prosedur dan proses,** yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan. Misalnya prosedur permohonan ijin akses aplikasi, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya.

**Kontrol dokumen**

Dokumen yang disyaratkan oleh ISMS harus dilindungi dan dikendalikan. Prosedur terdokumentasi harus ditetapkan untuk menetapkan tindakan manajemen yang diperlukan untuk:

* menyetujui dokumen untuk kecukupan sebelum diterbitkan;
* meninjau dan memperbarui dokumen sebagaimana diperlukan dan menyetujui kembali dokumen;
* memastikan bahwa perubahan dan status revisi dokumen saat ini diidentifikasi;
* memastikan bahwa versi relevan dari dokumen yang berlaku tersedia di tempat penggunaan;
* memastikan bahwa dokumen tetap terbaca dan mudah diidentifikasi;
* memastikan bahwa dokumen tersedia bagi mereka yang membutuhkannya, dan ditransfer, disimpan, dan pada akhirnya dibuang sesuai dengan prosedur yang berlaku untuk klasifikasi mereka;
* memastikan bahwa dokumen yang berasal dari luar diidentifikasi;
* memastikan bahwa distribusi dokumen dikendalikan;
* mencegah penggunaan dokumen usang yang tidak disengaja; dan
* menerapkan identifikasi yang sesuai kepada mereka jika mereka disimpan untuk tujuan apa pun.

**Kontrol catatan**

Rekaman harus dibuat dan dipelihara untuk memberikan bukti kesesuaian dengan persyaratan dan operasi efektif ISMS. Mereka harus dilindungi dan dikendalikan. ISMS harus memperhitungkan segala persyaratan hukum atau peraturan yang relevan dan kewajiban kontrak. Rekaman harus tetap terbaca, mudah diidentifikasi dan dapat diambil. Kontrol yang diperlukan untuk identifikasi, penyimpanan, perlindungan, pengambilan, waktu penyimpanan, dan disposisi catatan harus didokumentasikan dan diimplementasikan.

Rekaman harus disimpan dari kinerja proses sebagaimana diuraikan dalam 4.2 dan dari semua kejadian insiden keamanan yang signifikan terkait dengan ISMS.

CONTOH

Contoh catatan adalah buku pengunjung, laporan audit, dan formulir otorisasi akses yang sudah diisi

**Tanggung jawab**, yang dimaksud dengan tanggung jawab atau responsibility di sini adalah tercerminnya konsep dan aspek-aspek keamanan informasi perusahaan di dalam job description setiap jabatan dalam perusahaan. Begitu pula dengan adanya programprogram pelatihan serta pembinaan tanggung jawab keamaan informasi perusahaan untuk staf dan karyawannya.

 **Tanggung Jawab Manajemen,** Manajemen harus memberikan bukti komitmennya untuk pendirian, implementasi, operasi, pemantauan, peninjauan, pemeliharaan dan peningkatan ISMS dengan:

* menetapkan kebijakan ISMS;
* memastikan bahwa tujuan dan rencana SMKI ditetapkan;
* menetapkan peran dan tanggung jawab untuk keamanan informasi;
* mengkomunikasikan kepada organisasi pentingnya memenuhi tujuan keamanan informasi dan menyesuaikan dengan kebijakan keamanan informasi, tanggung jawabnya berdasarkan undang-undang dan kebutuhan untuk perbaikan berkelanjutan;
* menyediakan sumber daya yang cukup untuk membangun, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI (lihat 5.2.1);
* memutuskan kriteria untuk menerima risiko dan tingkat risiko yang dapat diterima;
* memastikan bahwa audit internal SMKI dilakukan (lihat 6); dan
* melakukan tinjauan manajemen terhadap SMKI (lihat 7).

**Sumber daya manusia**, adalah pelaksana serta obyek pengembangan keamanan informasi di perusahaan. Manusia yang bisa memperbaiki serta merusak semua usaha-usaha tersebut.

**Penyediaan sumber daya**

Organisasi harus menentukan dan menyediakan sumber daya yang dibutuhkan untuk:

* membangun, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan ISMS;
* memastikan bahwa prosedur keamanan informasi mendukung persyaratan bisnis;
* mengidentifikasi dan menangani persyaratan hukum dan peraturan dan kewajiban keamanan kontraktual;
* menjaga keamanan yang memadai dengan aplikasi yang benar dari semua kontrol yang diterapkan;
* melakukan tinjauan bila perlu, dan bereaksi secara tepat terhadap hasil tinjauan ini; dan
* jika diperlukan, meningkatkan efektivitas ISMS.

**Pelatihan, kesadaran dan kompetensi**

Organisasi harus memastikan bahwa semua personel yang diberi tanggung jawab yang ditetapkan dalam ISMS kompeten untuk melakukan tugas yang diminta dengan:

* menentukan kompetensi yang diperlukan untuk personel yang melakukan pekerjaan yang mempengaruhi ISMS;
* memberikan pelatihan atau mengambil tindakan lain (mis. mempekerjakan karyawan yang kompeten) untuk memenuhi kebutuhan ini;
* mengevaluasi efektivitas tindakan yang diambil; dan
* memelihara catatan pendidikan, pelatihan, keterampilan, pengalaman dan kualifikasi (lihat 4.3.3).

Organisasi juga harus memastikan bahwa semua personil yang relevan mengetahui relevansi dan pentingnya kegiatan keamanan informasi mereka dan bagaimana mereka berkontribusi terhadap pencapaian tujuan ISMS.

Lampiran A

(normatif)

Kontrol tujuan dan control

Tabel A.1 - Mengontrol tujuan dan control

|  |
| --- |
| A.5 Kebijakan keamanan  |
| A.5.1 Kebijakan keamanan informasiTujuan: Untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan persyaratan bisnis dan hukum dan peraturan yang relevan. |

|  |  |  |
| --- | --- | --- |
| A.5.1.1 | Kebijakan keamanan informasidokumen | KontrolDokumen kebijakan keamanan informasi harus disetujui olehmanajemen, dan diterbitkan serta dikomunikasikan kepada semua karyawandan pihak eksternal terkait. |
| A.5.1.2 | Tinjau informasikebijakan keamanan | KontrolKebijakan keamanan informasi harus ditinjau sesuai rencana interval atau jika perubahan signifikan terjadi untuk memastikan berlanjutnyakesesuaian, kecukupan, dan efektivitas. |
| A.6 Organisasi keamanan informasi |
| A.6.1 Organisasi internalTujuan: Untuk mengelola keamanan informasi dalam organisasi. |
| A.6.1.1 | Komitmen manajemen untukinformasi keamanan | KontrolManajemen harus secara aktif mendukung keamanan dalam organisasi melalui arah yang jelas, komitmen yang ditunjukkan, eksplisit penugasan, dan pengakuan keamanan informasitanggung jawab. |
| A.6.1.2 | Keamanan informasi bersamapentahbisan | KontrolKegiatan keamanan informasi harus dikoordinasikan oleh perwakilan dari berbagai bagian organisasi dengan yang relevanperan dan fungsi pekerjaan. |
| A.6.1.3 | Alokasi informasitanggung jawab keamanan | KontrolSemua tanggung jawab keamanan informasi harus didefinisikan dengan jelas. |
| A.6.1.4 | Proses otorisasi untukmemproses informasi fasilitas | KontrolProses otorisasi manajemen untuk informasi baru fasilitas pemrosesan harus didefinisikan dan diimplementasikan. |
| A.6.1.5 | Perjanjian kerahasiaan | KontrolPersyaratan untuk perjanjian kerahasiaan atau non-pengungkapanmencerminkan kebutuhan organisasi untuk perlindungan informasiharus diidentifikasi dan ditinjau secara berkala. |
| A.6.1.6 | Kontak dengan pihak berwenang | KontrolKontak yang sesuai dengan otoritas terkait harus dijaga. |
| A.6.1.7 | Kontak dengan minat khususKelompok | KontrolKontak yang sesuai dengan kelompok minat khusus atau spesialis lainnya forum keamanan dan asosiasi profesional harus dipertahankan. |
| A.6.1.8 | Tinjauan independen atasinformasi keamanan | KontrolPendekatan organisasi untuk mengelola keamanan informasi danimplementasinya (mis. mengontrol tujuan, kontrol, kebijakan, proses, dan prosedur untuk keamanan informasi) harus ditinjau secara independen pada interval yang direncanakan, atau ketika signifikan terjadi perubahan implementasi keamanan. |
| A.6.2 Pihak luarTujuan: Untuk menjaga keamanan informasi dan fasilitas pemrosesan informasi organisasi yang diakses, diproses, dikomunikasikan ke, atau dikelola oleh pihak eksternal. |
| A.6.2.1 | Identifikasi risiko yang terkaitkepada pihak eksternal  | KontrolRisiko terhadap informasi dan informasi organisasifasilitas pemrosesan dari proses bisnis yang melibatkan eksternalpara pihak harus diidentifikasi dan kontrol yang tepat dilaksanakansebelum memberikan akses. |
| A.6.2.2 | Mengatasi keamanan saat berurusan dengan pelanggan | KontrolSemua persyaratan keamanan yang diidentifikasi harus ditangani sebelum memberi pelanggan dapat mengakses informasi atau aset organisasi. |
| A.6.2.2 | Mengatasi keamanan di posisi ketiga perjanjian pihak | KontrolPerjanjian dengan pihak ketiga yang melibatkan pengaksesan, pemrosesan mengomunikasikan atau mengelola informasi organisasi atau fasilitas pemrosesan informasi, atau menambahkan produk atau layanan ke fasilitas pemrosesan informasi harus mencakup semua keamanan yang relevanPersyaratan. |
| A.7 Manajemen aset |
| A.7.1 Tanggung jawab atas asetTujuan: Untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi. |
| A.7.1.1 | Persediaan aset | KontrolSemua aset harus diidentifikasi secara jelas dan inventarisasi semua yang penting aset yang diambil dan dipelihara. |
| A.7.1.2 | Ownership of assets | KontrolSemua informasi dan aset terkait dengan pemrosesan informasi fasilitas harus 'dimiliki' 3 oleh bagian organisasi yang ditunjuk. |
| A.7.1.3 | Acceptable use of assets | KontrolAturan untuk penggunaan informasi dan aset terkait yang dapat diterimadengan fasilitas pemrosesan informasi harus diidentifikasi, didokumentasikan,dan diimplementasikan. |
| A.7.2 Klasifikasi informasiTujuan: Untuk memastikan bahwa informasi menerima tingkat perlindungan yang sesuai. |
| A.7.2.1 | Pedoman klasifikasi | KontrolInformasi harus diklasifikasikan berdasarkan nilainya, legalpersyaratan, sensitivitas, dan kekritisan terhadap organisasi. |
| A.7.2.2 | Pelabelan informasi danpenanganan | KontrolSerangkaian prosedur yang sesuai untuk pelabelan informasi danpenanganan harus dikembangkan dan diterapkan sesuai denganskema klasifikasi yang diadopsi oleh organisasi. |
| A.8 Keamanan sumber daya manusia |
| A.8.1 Sebelum bekerja Tujuan: Untuk memastikan bahwa karyawan, kontraktor, dan pengguna pihak ketiga memahami tanggung jawab mereka, dan sesuai untuk peran yang mereka pertimbangkan, dan untuk mengurangi risiko pencurian, penipuan, atau penyalahgunaan fasilitas. |
| A.8.1.2 | Peran dan tanggung jawab | KontrolPeran dan tanggung jawab keamanan karyawan, kontraktor dan pengguna pihak ketiga harus didefinisikan dan didokumentasikan sesuai dengan kebijakan keamanan informasi organisasi. |
| A.8.1.2. | Penyaringan | KontrolPemeriksaan verifikasi latar belakang pada semua kandidat untuk pekerjaan,kontraktor, dan pengguna pihak ketiga harus dilakukan sesuaidengan hukum, peraturan dan etika yang relevan, dan sebanding denganpersyaratan bisnis, klasifikasi informasi yang akandiakses, dan risiko yang dirasakan. |
| A.8.1.3 | Syarat dan ketentuanpekerjaan | KontrolSebagai bagian dari kewajiban kontrak mereka, karyawan, kontraktor dan pengguna pihak ketiga harus menyetujui dan menandatangani syarat dan ketentuan kontrak kerja mereka, yang akan menyatakan mereka dan tanggung jawab organisasi untuk keamanan informasi. |
| A.8.2 Selama bekerjaTujuan: Untuk memastikan bahwa semua karyawan, kontraktor, dan pengguna pihak ketiga mengetahui ancaman dan kekhawatiran keamanan informasi, tanggung jawab dan kewajiban mereka, dan diperlengkapi untuk mendukung kebijakan keamanan organisasi selama pekerjaan normal mereka, dan untuk mengurangi risiko manusia kesalahan. |
| A.8.2.1 | Tanggung jawab manajemen | Kontrol Manajemen harus mewajibkan karyawan, kontraktor, dan pihak ketiga pengguna untuk menerapkan keamanan sesuai dengan kebijakan yang ditetapkan dan prosedur organisasi. |
| A.8.2.2 | Informasi keamanankesadaran, pendidikan dan latihan | KontrolSemua karyawan organisasi dan, jika relevan, kontraktor dan pengguna pihak ketiga akan menerima pelatihan kesadaran yang tepat dan pembaruan rutin dalam kebijakan dan prosedur organisasi, seperti relevan untuk fungsi pekerjaan mereka. |
| A.8.2.3 | Proses pendisiplinan | KontrolAkan ada proses disipliner formal untuk karyawan yang memilikimelakukan pelanggaran keamanan |
| A.8.3 Pemutusan hubungan kerja atau perubahan pekerjaanTujuan: Untuk memastikan bahwa karyawan, kontraktor, dan pengguna pihak ketiga keluar dari organisasi atau berganti pekerjaan secara teratur. |
| A.8.3.1 | Tanggung jawab pemutusan hubungan kerja | KontrolTanggung jawab untuk melakukan pemutusan hubungan kerja atau perubahan pekerjaan harus didefinisikan dengan jelas dan ditugaskan. |
| A.8.3.2 | Pengembalian aset | KontrolSemua karyawan, kontraktor, dan pengguna pihak ketiga harus mengembalikan semua aset organisasi yang mereka miliki setelah pengakhiran aset mereka pekerjaan, kontrak atau perjanjian |
| A.8.3.3 | Penghapusan hak akses | KontrolHak akses semua karyawan, kontraktor, dan pengguna pihak ketigauntuk informasi dan fasilitas pemrosesan informasi harus dihapussetelah pemutusan hubungan kerja, kontrak atau perjanjian mereka, ataudisesuaikan saat perubahan |
| A.9 Keamanan fisik dan lingkungan |
| A.9.1 Area amanTujuan: Untuk mencegah akses fisik yang tidak sah, kerusakan, dan gangguan ke tempat dan informasi organisasi. |
| A.9.1.1 | Batas keamanan fisik | KontrolBatas keamanan (hambatan seperti dinding, entri yang dikendalikan kartu gerbang atau meja resepsionis berawak) harus digunakan untuk melindungi area yang memuat informasi dan fasilitas pemrosesan informasi. |
| A.9.1.2 | Kontrol entri fisik | KontrolArea aman harus dilindungi oleh kontrol entri yang sesuai untukmemastikan bahwa hanya personel yang berwenang yang diizinkan mengakses. |
| A.9.1.3 | Mengamankan kantor, kamar dan fasilitas | KontrolKeamanan fisik untuk kantor, kamar, dan fasilitas harus dirancangdan diterapkan. |
| A.9.1.4 | Melindungi dari luardan ancaman lingkungan | KontrolPerlindungan fisik terhadap kerusakan akibat kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil, dan bentuk alami atau buatan manusia lainnya bencana harus dirancang dan diterapkan. |
| A.9.1.5 | Bekerja di area yang aman | KontrolPerlindungan fisik dan pedoman untuk bekerja di area yang aman harus dirancang dan diterapkan. |
| A.9.1.6 | Akses publik, pengiriman danmemuat area | KontrolJalur akses seperti area pengiriman dan pemuatan dan titik lainnyadi mana orang yang tidak berwenang dapat memasuki tempat tersebut dikontrol dan, jika mungkin, diisolasi dari pemrosesan informasi fasilitas untuk menghindari akses tidak sah. |
| A.9.2 Keamanan peralatanTujuan: Untuk mencegah kehilangan, kerusakan, pencurian, atau kompromi aset dan gangguan pada kegiatan organisasi. |
| A.9.2.1 | Penentuan letak peralatan danperlindungan | ControlPeralatan harus diletakkan atau dilindungi untuk mengurangi risiko dariancaman dan bahaya lingkungan, dan peluang untukakses yang tidak sah. |
| A.9.2.2 | Utilitas pendukung | KontrolPeralatan harus dilindungi dari kegagalan daya dan lainnyagangguan yang disebabkan oleh kegagalan dalam utilitas pendukung. |
| A.9.2.3 | Keamanan kabel | KontrolKabel listrik dan telekomunikasi yang membawa data atau pendukung layanan informasi harus dilindungi dari intersepsi atau kerusakan |
| A.9.2.4 |  Perawatan peralatan | KontrolPeralatan harus dipelihara dengan benar untuk memastikan kelanjutannya ketersediaan dan integritas |
| A.9.2.5 | Keamanan peralatan tempat |  KontrolKeamanan harus diterapkan pada peralatan di luar lokasi dengan mempertimbangkan berbagai risiko bekerja di luar gedung organisasi. |
| A.9.2.6 | Pembuangan atau penggunaan kembali yang aman dariperalatan | KontrolSemua item peralatan yang mengandung media penyimpanan harus diperiksa memastikan bahwa data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa dengan aman sebelum dibuang |
| A.9.2.7 | Penghapusan properti | KontrolPeralatan, informasi atau perangkat lunak tidak boleh dibawa keluar-situs tanpa otorisasi sebelumnya |
| A.10.1 Prosedur dan tanggung jawab operasional |
| Tujuan: Untuk memastikan operasi fasilitas pemrosesan informasi yang benar dan aman |
| A.10.7.1 | Manajemen dilepas media | Kontrol Harus ada prosedur untuk manajemen media yang bisa dipindahkan. |
| A.10.7.2 | Pembuangan media | KontrolMedia harus dibuang dengan aman dan aman ketika tidak lagi diperlukan, menggunakan prosedur formal. |
| A.10.7.3 | Penanganan informasiProsedur | KontrolProsedur untuk penanganan dan penyimpanan informasi harusdidirikan untuk melindungi informasi ini dari pengungkapan yang tidak sah atau penyalahgunaan. |
| A.10.7.4 | Keamanan sistem dokumentasi |
|  |  |
| A.10.8 Pertukaran informasiTujuan: Untuk menjaga keamanan informasi dan perangkat lunak yang dipertukarkan dalam suatu organisasi dan dengan entitas eksternal apa pun. |
| A.10.8.1 | Pertukaran informasikebijakan dan prosedur | KontrolKebijakan, prosedur, dan kontrol pertukaran formal harus adauntuk melindungi pertukaran informasi melalui penggunaan semua jenis fasilitas komunikasi |
| A.10.8.2 | Perjanjian pertukaran | KontrolPerjanjian harus dibuat untuk pertukaran informasi dan perangkat lunak antara organisasi dan pihak eksternal. |
| A.10.8.3 | Media fisik dalam perjalanan | KontrolMedia yang mengandung informasi harus dilindungi akses tidak sah, penyalahgunaan atau korupsi selama transportasimelampaui batas fisik organisasi |
| A.10.8.4 | Olahpesan elektronik |  Kontrol Informasi yang terlibat dalam pengiriman pesan elektronik harus tepat terlindung |
| A.10.8.5 | Informasi bisnis sistem | KontrolKebijakan dan prosedur harus dikembangkan dan diterapkan untukmelindungi informasi yang terkait dengan interkoneksi bisnissistem Informasi. |
| A.10.9 Layanan perdagangan elektronikTujuan: Untuk memastikan keamanan layanan perdagangan elektronik, dan penggunaannya yang aman. |
| A.10.9.1 | Perdagangan elektronik | KontrolInformasi yang terlibat dalam perdagangan elektronik melewati publik jaringan harus dilindungi dari aktivitas penipuan, sengketa kontrak, dan pengungkapan dan modifikasi yang tidak sah |
| A.10.9.2 | Transaksi online | KontrolInformasi yang terlibat dalam transaksi online harus dilindungimencegah pengiriman yang tidak lengkap, salah rute, tidak diotorisasi perubahan pesan, pengungkapan yang tidak sah, pesan yang tidak sah duplikasi atau ulangan. |
| A.10.9.3 | Tersedia untuk umuminformasi | KontrolIntegritas informasi dibuat tersedia untuk umum sistem yang tersedia harus dilindungi untuk mencegah tidak sahmodifikasi. |
| A.10.10 PemantauanTujuan: Untuk mendeteksi kegiatan pemrosesan informasi yang tidak sah. |
| A.10.10.1 | Log masuk audit | KontrolLog audit mencatat aktivitas pengguna, pengecualian, dan informasi peristiwa keamanan harus diproduksi dan disimpan untuk jangka waktu yang disepakati untuk membantu dalam penyelidikan di masa depan dan pemantauan kontrol akses |
| A.10.10.2 | penggunaan sistem pemantauan | KontrolProsedur untuk memantau penggunaan fasilitas pemrosesan informasi harus ditetapkan dan hasil dari kegiatan pemantauanditinjau secara teratur |
| A.10.10.3 | Perlindungan informasi log | KontrolFasilitas logging dan informasi log harus dilindungi merusak dan mengakses tanpa izin. |
| A.10.10.4 | Administrator dan operatorlog | KontrolAdministrator sistem dan aktivitas operator sistem harus dicatat. |
| A.10.10.5 | Kesalahan logging | KontrolAdministrator sistem dan aktivitas operator sistem harus dicatat. |
| A.10.10.6 | Sinkronisasi jam | KontrolJam dari semua sistem pemrosesan informasi yang relevan dalam suatu organisasi atau domain keamanan harus disinkronkan dengan menyetujui sumber waktu yang akurat. |
| A.11 Kontrol akses |
| A.11.1 Persyaratan bisnis untuk kontrol aksesTujuan: Untuk mengontrol akses ke informasi |
| A.11.1.1 | Kebijakan kontrol akses | KontrolKebijakan kontrol akses harus ditetapkan, didokumentasikan, dan ditinjau berdasarkan persyaratan bisnis dan keamanan untuk akses. |
| A.11.2 Manajemen akses penggunaTujuan: Untuk memastikan akses pengguna yang sah dan untuk mencegah akses yang tidak sah ke sistem informasi. |
| A.11.10.1 | Pendaftaran pengguna | KontrolAkan ada registrasi pengguna formal dan de-registrasiprosedur di tempat untuk memberikan dan mencabut akses ke semua sistem dan layanan informasi |
| A.11.10.2 | Manajemen hak istimewa | KontrolAlokasi dan penggunaan hak istimewa akan dibatasi dan |
| A.11.10.3 | Manajemen kata sandi pengguna | KontrolAlokasi kata sandi harus dikontrol melalui formalproses manajemen. |
| A.11.10.4 | Tinjau hak akses pengguna | KontrolManajemen akan meninjau hak akses pengguna secara berkalamenggunakan proses forma |
| A.11.3 Tanggung jawab penggunaTujuan: Untuk mencegah akses pengguna yang tidak sah, dan kompromi atau pencurian informasi dan fasilitas pemrosesan informasi. |
| A.11.3.1 | Penggunaan kata sand | KontrolPengguna harus mengikuti praktik keamanan yang baik di pemilihan dan penggunaan kata sandi. |
| A.11.3.2 | Peralatan pengguna tanpa pengawasan | KontrolPengguna harus memastikan bahwa peralatan tanpa pengawasan telah sesuai perlindungan |
| A.11.3.3 | Meja yang jelas dan layar yang jelas kebijakan | KontrolKebijakan meja yang jelas untuk kertas dan media penyimpanan yang dapat dilepas dan kebijakan layar yang jelas untuk fasilitas pemrosesan informasi harusdiadopsi. |
| A.11.4 Kontrol akses jaringanTujuan: Untuk mencegah akses tidak sah ke layanan jaringan. |
| A.11.4.1 | Kebijakan tentang penggunaan jaringan | Kontrol Pengguna hanya akan diberikan akses ke layanan yang mereka miliki telah secara khusus diizinkan untuk digunakan |
| A.11.4.2 | Otentikasi pengguna untukkoneksi eksterna | KontrolMetode otentikasi yang sesuai harus digunakan untuk mengontrol akses oleh pengguna jarak jauh |
| A.11.4.3 | Identifikasi peralatan dijaringan | KontrolIdentifikasi peralatan otomatis harus dianggap sebagai saranauntuk mengotentikasi koneksi dari lokasi dan peralatan tertentu. |
| A.11.4.4 | Diagnosis jarak jauh dankonfigurasi port konfiguras | KontrolAkses fisik dan logis ke port diagnostik dan konfiguras |
| A.11.4.5 | Pemisahan dalam jaringan | KontrolKelompok layanan informasi, pengguna, dan sistem informasi wajib dipisahkan pada jaringan |
| A.11.4.6 | Kontrol koneksi jaringan | KontrolUntuk jaringan bersama, terutama yang membentang di Internetbatas organisasi, kemampuan pengguna untuk terhubung ke Internetjaringan harus dibatasi, sejalan dengan kebijakan kontrol akses danpersyaratan aplikasi bisnis |
| A.11.4.7 | Kontrol perutean jaringan | KontrolKontrol perutean harus diterapkan untuk jaringan untuk memastikan hal itukoneksi komputer dan arus informasi tidak melanggarkebijakan kontrol akses aplikasi bisnis |
| A.11.5 Kontrol akses sistem operasiTujuan: Untuk mencegah akses tidak sah ke sistem operasi. |
| A.11.5.1 | Prosedur masuk yang aman | KontrolAkses ke sistem operasi harus dikontrol oleh log-on yang aman prosedur |
| A.11.5.2 | Identifikasi pengguna danotentikasi | KontrolSemua pengguna harus memiliki pengidentifikasi unik (ID pengguna untuk pribadi mereka hanya menggunakan, dan teknik otentikasi yang sesuai harus dipilih membuktikan identitas yang diklaim pengguna. |
| A.11.5.3 | Manajemen kata sandi sistem | KontrolSistem untuk mengelola kata sandi harus interaktif dan harus memastikan kata sandi yang berkualitas. |
| A.11.5.4 | Penggunaan utilitas sistem | KontrolPenggunaan program utilitas yang mungkin mampu mengesampingkan kontrol sistem dan aplikasi harus dibatasi dan ketat dikontrol. |
| A.11.5.5 | sistem Batas waktu sesi | KontrolSesi tidak aktif harus ditutup setelah periode tidak aktif yang ditentukan |
| A.11.5.6 | Batasan waktu koneksi | KontrolPembatasan waktu koneksi harus digunakan untuk memberikan tambahan keamanan untuk aplikasi berisiko tinggi. |
| A.11.6 Kontrol akses aplikasi dan informasiTujuan: Untuk mencegah akses tidak sah ke informasi yang disimpan dalam sistem aplikasi. |
| A.11.6.1 | Akses informasi larangan | KontrolAkses ke informasi dan fungsi sistem aplikasi oleh pengguna danpersonel pendukung harus dibatasi sesuai dengan yang ditentukankebijakan kontrol akses. |
| A.11.6.2 | Isolasi sistem yang sensiti | KontrolAkses ke informasi dan fungsi sistem aplikasi oleh pengguna danpersonel pendukung harus dibatasi sesuai dengan yang ditentukankebijakan kontrol akses. |
| A.11.7 Komputasi dan teleworking selulerTujuan: Untuk memastikan keamanan informasi saat menggunakan komputasi bergerak dan fasilitas teleworking. |
| A.11.7.1 | Komputasi seluler dankomunikasi | Kontrol Kebijakan formal harus ada, dan langkah-langkah keamanan yang sesuai harus diadopsi untuk melindungi terhadap risiko menggunakan ponsel fasilitas komputasi dan komunikasi |
| A.11.7.2 | Teleworking | KontrolSuatu kebijakan, rencana dan prosedur operasional harus dikembangkan dan diimplementasikan untuk kegiatan teleworking. |
| A.12 Pengambilan, pengembangan dan pemeliharaan sistem informas |
| A.12.1 Persyaratan keamanan sistem informasiTujuan: Untuk memastikan bahwa keamanan adalah bagian integral dari sistem informasi. |
| A.12.1 | Persyaratan keamanananalisis dan spesifikasi | KontrolPernyataan persyaratan bisnis untuk sistem informasi baru atau peningkatan pada sistem informasi yang ada harus menentukan persyaratan untuk kontrol keamanan. |
| A.12.2 Pemrosesan yang benar dalam aplikasiTujuan: Untuk mencegah kesalahan, kehilangan, modifikasi yang tidak sah, atau penyalahgunaan informasi dalam aplikasi. |
| A.12.2.1 | Input validasi data | Kontrol Input data ke aplikasi harus divalidasi untuk memastikan bahwa data ini benar dan tepat |
| A.12.2.2 | Input validasi data Kontrol internal pengolahan | KontrolPemeriksaan validasi harus dimasukkan ke dalam aplikasi untuk dideteksi segala korupsi informasi melalui kesalahan pemrosesan atau disengaja tindakan. |
| A.12.2.3 | Integritas pesan | KontrolPersyaratan untuk memastikan keaslian dan melindungi pesanintegritas dalam aplikasi harus diidentifikasi, dan kontrol yang sesuai diidentifikasi dan diimplementasikan |
| A.12.2.4 | Validasi data keluaran | KontrolOutput data dari aplikasi harus divalidasi untuk memastikan bahwa pemrosesan informasi yang disimpan adalah benar dan sesuai untuk keadaan. |
| A.12.3 Kontrol kriptografiTujuan: Untuk melindungi kerahasiaan, keaslian, atau integritas informasi dengan cara kriptografi |
| A.12.3.1 | Kebijakan tentang penggunaankontrol kriptograf | KontrolKebijakan penggunaan kontrol kriptografi untuk perlindunganinformasi harus dikembangkan dan diimplementasikan |
| A.12.3.2 | Manajemen kunci | KontrolManajemen kunci harus ada untuk mendukung penggunaan organisasiteknik kriptograf |
| A.12.4 Keamanan file sistemTujuan: Untuk memastikan keamanan file sistem. |
| A.12.4.1 | Kontrol operasionalperangkat lunak | KontrolHarus ada prosedur untuk mengontrol instalasiperangkat lunak pada sistem operasional |
| A.12.4.2 | Perlindungan uji sistemdata | KontrolData uji harus dipilih dengan hati-hati, dan dilindungi serta dikendalikan |
| A.12.4.3 | Kontrol akses ke programKode sumber | KontrolAkses ke kode sumber program harus dibatasi. |
| A.12.5 Keamanan dalam proses pengembangan dan dukunganTujuan: Untuk menjaga keamanan perangkat lunak dan informasi sistem aplikasi. |
| A.12.5.1 | Ubah prosedur kontrol | KontrolImplementasi perubahan harus dikendalikan oleh penggunaanprosedur kontrol perubahan forma |
| A.12.5.2 | Ulasan teknis setelah operasiperubahan sistem | KontrolKetika sistem operasi diubah, aplikasi bisnis penting harus ditinjau dan diuji untuk memastikan tidak ada dampak burukpada operasi atau keamanan organisasi |
| A.12.5.3 | Batasan pada perubahan menjadi paket perangkat lunak | KontrolModifikasi pada paket perangkat lunak harus dicegah, terbatas pada perubahan yang diperlukan, dan semua perubahan harus dikontrol dengan ketat |
| A.12.5.4 | Kebocoran informasi | KontrolPeluang untuk kebocoran informasi harus dicegah. |
| A.12.5.5 | Perangkat lunak outsourcingpengembangan | KontrolPengembangan perangkat lunak outsourcing akan diawasi dandipantau oleh organisas |

**Serial ISO 27000**

International Standards Organization (ISO) mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, seperti pada serial ISO 27000. Adapun beberapa standar di seri ISO ini adalah sebagai berikut:

**ISO 27000:** dokumen defenisi-defenisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.

**ISO 27001**: berisi aspek-aspek pendukung realisasi serta implementasi sistem manajemen keamanan informasi perusahaan

**ISO 27002**: terkait dengan dokumen ISO 27001, namun dalam dokumen ini terdapat panduan praktis pelaksanaan dan implementasi sistem manajemen keamanan informasi perusahaan.

**ISO 27003**: panduan implementasi sistem manajemen keamanan informasi perusahaan.

**ISO 27004**: dokumen yang berisi matriks dan metode pengukuran keberhasilan implementasi sistem manajemen keamanan informasi.

**ISO 27005**: dokumen panduan pelaksanaan manajemen risiko.

**ISO 27006**: dokumen panduan untuk sertifikasi sistem manajemen keamanan informasi perusahaan.

**ISO 27007**: dokumen panduan audit sistem manajemen keamanan informasi perusahaan.

**ISO 27799**: panduan ISO 27001 untuk industri kesehatan.

 ISO 27001: 2005 digunakan sebagai icon sertifikasi ISO 27000.ISO 27001: 2005 merupakan dokumen standar sistem manajemen keamanan informasi atau *Information Security Managemen System*–ISMS yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka mengimplementasikan konsep-konsep keamanan informasi di perusahaan. Secara umum ada 11 aspek atau yang biasa disebut sebagai *control*, yang harus ada dalam setiap perusahaan dalam usahanya mengimplementasikan konsep keamanan informasi.

 Control dalam hal ini adalah hal-hal, bisa berupa proses, prosedur, kebijakan maupun *tool* yang digunakan sebagai alat pencegahan terjadinya sesuatu yang tidak dikehendaki oleh adanya konsep keamanan informasi, seperti akses terlarang terhadap data atau informasi rahasia perusahaan.

**Bagaimana ISO/IEC 27001:2005 Dijalankan**

Penilaian risiko dan manajemen yang benar adalah faktor terpenting dalam ISO/IEC 27001. Standar ini membolehkan organisasi memperkenalkan objek-objek pengawasan dan memilih cara-cara penyelenggaraan keamanan yang paling sesuai. Jika organisasi ingin memulai menerapkan standard ini, maka mulai dengan mendefinisikan semua permasalahan dan faktor-faktor yang terkait secara sistematik dan cara-cara manajemen risiko yang sudah atau akan diterapkan (direncanakan).

Pendefenisian ini bertujuan untuk memberikan pendekatan terhadap pengelolaan (manajemen) risiko yang akan ditetapkan dalam bentuk aturan-aturan, terkait dengan penilaian risiko oleh tim auditor (fihak organisasi sendiri atau konsultan yang memahami standar ini) untuk memastikan peringkat keamanan yang diperlukan sesuai dengan kondisi anggaran keuangan organisasi.

Objek-objek dan cara-cara kontrolnya dapat dilihat pada lampiran ISO/IEC 27001:2005 agar dapat mencapai keperluan-keperluan yang diperkenalkan (hasil maksimal yang diharapkan) dalam penilaian risiko dan proses pemulihannya. Jika sistem keamanan yang telah diwujudkan sudah sampai taraf memuaskan, maka kontrol yang diuraikan dalam lampiran dapat diabaikan. Kontrol dan evaluasi yang ekstra ketat dapat juga diterapkan. Setelah mampu mengimplementasikan manajemen risiko yang tersistematis, organisasi dapat menetapkan bahwa sistemnya telah sesuai untuk keperluan-keperluan sendiri dan standard.

**11 Domain ISO 27001**

ISO 27001 memiliki 11 Domain, 39 Control Objectives 133 Security Controls. Controls tersebut disebutkan didalam dokumen ISO 27001 Annex A Controls. Dan juga telah disebutkan domain yang digunakan dalam ISO 27001.

Annex A berisi control sebagai berikut (Biasanya disebut dengan ISO 27001 Annex A Domains):

* A.5 Security policy
* A.6 Organization of information security
* A.7 Asset management
* A.8 Human resources security
* A.9 Physical and environmental security
* A.10 Communications and operations management
* A.11 Access control
* A.12 Information systems acquisition, development and maintenance
* A.13 Information security incident management
* A.14 Business continuity management
* A.15 Compliance
1. **Security Policy (**Kebijakan Keamanan)

Tujuan utama dari control ini adalah memastikan adanya arahan manajerial serta dukungan eksekutif perusahaan terhadap semua usaha yang terkait dengan pembangunan serta pengimplementasian konsep-konsep keamanan informasi. Di samping itu, kebijakan keamanan ini juga digunakan sebagai jaminan bahwa semua usaha tersebut telah sesuai dengan kebutuhan- kebutuhan bisnis.

**Apa yang seharusnya terkandung dalam Kebijakan Keamanan Informasi?**

ISO 27001 tidak mengatakan terlalu banyak tentang kebijakan tersebut, tetapi ia mengatakan hal berikut:

* Kebijakan tersebut perlu disesuaikan dengan organisasi - ini berarti Anda tidak bisa begitu saja menyalin kebijakan dari perusahaan manufaktur besar dan menggunakannya di perusahaan IT kecil.
* Perlu mendefinisikan kerangka kerja untuk menetapkan tujuan keamanan informasi - pada dasarnya, kebijakan perlu menentukan bagaimana tujuan diusulkan, bagaimana mereka disetujui, dan bagaimana mereka ditinjau. Lihat juga: Tujuan kontrol ISO 27001 - Mengapa penting?
* Kebijakan tersebut harus menunjukkan komitmen manajemen puncak untuk memenuhi persyaratan semua pihak yang berkepentingan, dan untuk terus meningkatkan ISMS - ini biasanya dilakukan melalui semacam pernyataan di dalam kebijakan.
* Kebijakan tersebut harus dikomunikasikan dalam perusahaan, tetapi juga - jika perlu - kepada pihak yang berkepentingan; Praktik terbaik adalah menentukan siapa yang bertanggung jawab untuk komunikasi semacam itu, dan kemudian orang itu bertanggung jawab untuk melakukannya terus-menerus.
* Kebijakan harus ditinjau secara berkala - pemilik kebijakan harus ditetapkan, dan orang ini bertanggung jawab untuk memperbarui kebijakan tersebut.

Jadi, seperti yang Anda lihat, kebijakan tersebut tidak harus berupa dokumen yang sangat panjang. Dan tidak, Anda tidak harus memasukkan semua aturan keamanan informasi dalam dokumen ini - untuk tujuan itu Anda akan menulis kebijakan terperinci seperti Kebijakan Kontrol Akses, Kebijakan Klasifikasi, Kebijakan Penggunaan yang Dapat Diterima, dll.

**Apa yang bisa Anda sertakan**

Meskipun tidak wajib, jika Anda adalah perusahaan yang lebih kecil Anda juga dapat memasukkan yang berikut (untuk perusahaan yang lebih besar, masalah ini biasanya didokumentasikan secara terpisah):

* Ruang lingkup ISMS - dengan cara ini ruang lingkup tidak harus ada sebagai dokumen terpisah.
* Tanggung jawab untuk bagian-bagian penting dari SMKI - mis., Yang bertanggung jawab atas operasi dan koordinasi sehari-hari, siapa yang bertanggung jawab pada tingkat eksekutif, siapa yang bertanggung jawab untuk penilaian risiko, untuk insiden, audit internal, dll.
* Pengukuran - siapa yang akan mengukur apakah tujuan keamanan informasi telah tercapai, kepada siapa hasil perlu dilaporkan, seberapa sering, dll. (Lihat juga: Cara melakukan pemantauan dan pengukuran dalam ISO 27001)

Di beberapa perusahaan besar, saya telah melihat Kebijakan Keamanan Informasi bergabung dengan Kebijakan Manajemen Risiko Perusahaan. Meskipun ini tidak salah, saya pikir lebih baik untuk menjaga kebijakan ini sebagai dokumen terpisah - fokusnya tetap lebih jelas.

**Input yang dibutuhkan**

Ada beberapa input yang harus Anda perhitungkan saat menulis kebijakan:

* Niat manajemen puncak dengan keamanan informasi - hal terbaik adalah menjadwalkan wawancara dengan CEO Anda dan menelusuri semua elemen kebijakan; Anda mungkin mengiriminya email beberapa hari sebelum rapat, sehingga ia punya waktu untuk memikirkannya.
* Peraturan perundang-undangan dan persyaratan kontrak - kebijakan Anda harus mencerminkan itu.
* Sistem yang ada untuk menetapkan tujuan - jika sistem tersebut ada, Anda harus merujuknya.

**Mulailah melihat kebijakan ini dengan cara yang berbeda**

Jadi intinya adalah - Kebijakan Keamanan Informasi harus benar-benar berfungsi sebagai penghubung utama antara manajemen puncak Anda dan kegiatan keamanan informasi Anda, terutama karena ISO 27001 mensyaratkan manajemen untuk memastikan bahwa SMKI dan tujuannya sesuai dengan arahan strategis perusahaan ( klausul 5.2 dari ISO 27001). Kebijakan ini mungkin merupakan cara terbaik untuk melakukan ini.

Jadi, Anda harus membuat kebijakan ini singkat dan dapat dimengerti oleh manajemen puncak Anda. Dan tolong jangan menulis dokumen panjang 80 halaman yang mencoba menjelaskan semua aturan keamanan informasi - ini adalah cara terbaik untuk membuat dokumen yang tidak akan pernah dibaca oleh siapa pun.

1. **Organization of Information Security (Organisasi Keamanan Informasi)**

Control ini bertujuan utama antara lain untuk:

– Memastikan pengelolaan serta integrasi konsep keamanan informasi dalam organisasi, baik dalam bentuk keberadaan fungsi keamanan dalam organisasi maupun integrasi dengan proses bisnis dan tanggung jawab sumber daya manusia.
– Memastikan terjaminnya keamanan informasi pada situasi serta kondisi dimana pihak eksternal terlibat dalam satu atau lebih proses bisnis perusahaan.

Peran & Tanggung Jawab Keamanan Informasi

Semua tanggung jawab keamanan informasi perlu didefinisikan dan dialokasikan. Tanggung jawab keamanan informasi dapat bersifat umum (mis. Melindungi informasi) dan / atau spesifik (mis. Tanggung jawab untuk memberikan izin tertentu). Pertimbangan harus diberikan pada kepemilikan aset informasi atau kelompok aset saat mengidentifikasi tanggung jawab. Beberapa contoh peran bisnis yang cenderung memiliki relevansi keamanan informasi meliputi; Kepala departemen; Pemilik proses bisnis; Manajer fasilitas; Manajer HR; dan Auditor Internal. Auditor akan mencari untuk mendapatkan kepastian bahwa organisasi telah menjelaskan siapa yang bertanggung jawab atas apa yang secara memadai dan proporsional sesuai dengan ukuran dan sifat organisasi. Untuk organisasi yang lebih kecil, umumnya tidak realistis untuk memiliki peran penuh waktu yang terkait dengan peran dan tanggung jawab ini. Karena itu, mengklarifikasi tanggung jawab keamanan informasi spesifik dalam peran pekerjaan yang ada adalah penting, mis. Direktur Operasi atau CEO mungkin juga setara dengan CISO, Kepala Petugas Keamanan Informasi, dengan tanggung jawab menyeluruh atas semua SMKI. CTO mungkin memiliki semua aset informasi terkait teknologi, dll.

Pemisahan Tugas

Tugas dan bidang tanggung jawab yang saling bertentangan harus dipisahkan untuk mengurangi peluang untuk modifikasi yang tidak sah atau tidak disengaja atau penyalahgunaan aset organisasi. Organisasi perlu bertanya pada dirinya sendiri apakah pemisahan tugas telah dipertimbangkan dan dilaksanakan jika perlu. Organisasi yang lebih kecil mungkin berjuang dengan ini, tetapi prinsipnya harus diterapkan sejauh mungkin dan tata kelola & kontrol yang baik diterapkan untuk aset informasi risiko / nilai yang lebih tinggi, yang ditangkap sebagai bagian dari evaluasi dan perawatan risiko.

Kontak dengan Pihak Berwenang

Kontak yang sesuai dengan otoritas terkait harus dijaga. Ingat ketika mengadaptasi kontrol ini untuk memikirkan tentang tanggung jawab hukum untuk menghubungi pihak berwenang seperti Polisi, Kantor Komisaris Informasi atau badan pengatur lainnya, mis. sekitar GDPR. Pertimbangkan bagaimana kontak itu dibuat, oleh siapa, dalam keadaan apa, dan sifat informasi yang akan diberikan

Kontak dengan Kelompok Minat Khusus

Kontak yang sesuai dengan kelompok minat khusus atau forum keamanan spesialis lainnya dan asosiasi profesional juga harus dijaga. Ketika mengadaptasi kontrol ini untuk kebutuhan spesifik Anda, ingatlah bahwa keanggotaan badan profesional, organisasi industri, forum, dan kelompok diskusi semuanya diperhitungkan dalam kontrol ini. Penting untuk memahami sifat masing-masing kelompok ini dan untuk tujuan apa mereka dibentuk (mis. Apakah ada tujuan komersial di baliknya).

Keamanan Informasi dalam Manajemen Proyek

Keamanan informasi perlu ditangani dalam manajemen proyek, terlepas dari jenis proyek. Keamanan Informasi harus tertanam dalam jalinan organisasi dan manajemen proyek adalah bidang utama untuk ini. Kami merekomendasikan penggunaan kerangka kerja kerangka kerja untuk proyek yang menyertakan daftar periksa berulang sederhana untuk menunjukkan bahwa keamanan informasi sedang dipertimbangkan. Auditor akan mencari untuk melihat bahwa semua orang yang terlibat dalam proyek ditugaskan untuk mempertimbangkan keamanan informasi pada semua tahap siklus hidup proyek sehingga ini juga harus dibahas sebagai bagian dari pendidikan dan kesadaran sejalan dengan Keamanan SDM untuk A.7.2.2 .

Organisasi cerdas juga akan memenuhi A.6.1.5 dengan kewajiban terkait untuk data pribadi dan mempertimbangkan keamanan dengan desain bersama dengan Penilaian Dampak Perlindungan Data (DPIA) dan proses serupa untuk menunjukkan kepatuhan terhadap Peraturan Perlindungan Data Umum (GDPR) dan Undang-Undang Perlindungan Data 2018.

1. **Asset Management (Manajemen Aset)**

Control ini memastikan bahwa perusahaan sudah mengidentifikasi semua asset informasinya, siapa yang memiliki atau bertanggung jawab terhadap aset tersebut dan bagaimana proses serta prosedur yang sesuai dalam kegiatan pengelolaan dan penggunaan informasi tersebut. Di samping itu, juga perlu dipastikan adanya control yang mampu mengklasifikasikan jenis-jenis data dan informasi serta bagaimana pengelolaannya untuk setiap klasifikasi.

Apa tujuan Lampiran A.8.1 dari ISO 27001: 2013?

Lampiran A.8.1 adalah tentang tanggung jawab atas aset. Tujuan dalam Lampiran ini adalah untuk mengidentifikasi aset informasi dalam ruang lingkup sistem manajemen dan menentukan tanggung jawab perlindungan yang sesuai. Ini adalah bagian penting dari sistem manajemen keamanan informasi (ISMS) terutama jika Anda ingin mencapai sertifikasi ISO 27001. Mari kita memahami persyaratan itu dan apa artinya sedikit lebih dalam sekarang.

Inventarisasi Aset

Aset apa pun yang terkait dengan informasi dan fasilitas pemrosesan informasi perlu diidentifikasi dan dikelola selama siklus hidup, selalu mutakhir. Daftar atau inventaris aset-aset tersebut harus disatukan yang menunjukkan bagaimana mereka dikelola dan dikendalikan, berdasarkan kepentingannya (yang juga cocok dengan klasifikasi informasi di bawah). Siklus hidup informasi ini umumnya mencakup tahap pembuatan, pemrosesan, penyimpanan, transmisi, penghapusan, dan penghancuran.

1. **Human Resources Security (Keamanan Sumber Daya Manusia**

Control berkaitan erat dengan pengelolaan sumber daya manusia di dalam sebuah perusahaan. Manusia adalah ancaman terbesar dari keamanan informasi dan staf atau karyawan yang bekerja di dalam sebuah perusahaan adalah ancaman yang lebih besar bagi keamanan informasi di dalam perusahaan tersebut. Seperti kejadian di atas terkait dengan penyalahgunaan e-mail. Prosedur serta proses harus dimiliki perusahaan terkait dengan proses penerimaan karyawan, seperti interview dan screening; tanggung jawab karyawan selama dan ketika akan resign dari perusahaan tempatnya bekerja.

Pemutaran

Kontrol yang baik mencakup verifikasi latar belakang dan pemeriksaan kompetensi pada semua kandidat untuk pekerjaan. Ini harus dilakukan sesuai dengan undang-undang, peraturan dan etika yang relevan, dan harus proporsional dengan persyaratan bisnis, klasifikasi informasi yang akan diakses dan risiko yang dirasakan terkait. Misalnya, staf yang mengakses aset informasi tingkat lebih tinggi yang memiliki risiko lebih tinggi dapat dikenakan pemeriksaan yang jauh lebih ketat daripada staf yang hanya pernah mendapatkan akses ke informasi publik atau menangani aset dengan ancaman terbatas. Menempatkan kontrol SDM yang memadai dan proporsional di semua tahap pekerjaan membantu mengurangi kemungkinan ancaman kecelakaan atau berbahaya. Penyaringan juga harus dilakukan untuk kontraktor (kecuali organisasi induk mereka memenuhi kontrol keamanan Anda yang lebih luas misalnya memiliki ISO 27001 sendiri dan melakukan pemeriksaan latar belakang mereka sendiri). Seorang auditor akan berharap untuk melihat proses penyaringan dengan prosedur yang jelas dioperasikan secara konsisten setiap kali juga membantu menghindari risiko preferensi / prasangka juga. Idealnya ini akan diselaraskan dengan keseluruhan proses perekrutan organisasi.

Syarat & Ketentuan Pekerjaan

Perjanjian kontrak dengan karyawan dan kontraktor harus menyatakan tanggung jawab mereka dan organisasi untuk keamanan informasi. Perjanjian-perjanjian ini adalah tempat yang baik untuk menempatkan tanggung jawab utama keamanan informasi dan umum individu karena mereka memiliki bobot hukum - yang berarti mereka didukung oleh hukum. Ini juga sangat penting sehubungan dengan GDPR dan Undang-Undang Perlindungan Data baru 2018. Mereka harus merujuk dan mencakup seluruh jajaran area kontrol termasuk kepatuhan keseluruhan terhadap ISMS serta penggunaan yang lebih spesifik yang dapat diterima, kepemilikan HKI, pengembalian aset dll. Kami merekomendasikan bekerja dengan Pengacara SDM jika Anda tidak yakin karena konsekuensi untuk mendapatkan kontrak kerja yang salah dari perspektif keamanan informasi (dan dimensi lainnya) dapat menjadi signifikan.

1. **Physical and Environmental Security (Keamanan Fisik dan Lingkungan)**

Control ini terdiri dari aspek-aspek berikut:

– Pengamanan area tempat kerja perusahaan yang diwujudkan, misalnya dengan adanya tool seperti biometrics security berupa sidik jari maupun name tag karyawan. Ini juga termasuk pada bagaimana seharusnya akses ke dalam data center akan dilakukan.
– Penempatan serta akses terhadap alat kerja perusahaan, seperti telepon, printer, PC, dan lain sebagainya, sedemikian rupa sehingga hanya bisa digunakan oleh karyawan perusahaan saja.

Area aman

Tujuan dari kategori ini adalah untuk mencegah akses fisik yang tidak sah, kerusakan atau gangguan pada bangunan dan infrastruktur rumah sakit, menggunakan kontrol yang sesuai dengan risiko yang teridentifikasi dan nilai aset yang dilindungi.

Batas keamanan fisik • Batas keamanan harus digunakan untuk melindungi area yang berisi informasi dan fasilitas pemrosesan informasi - menggunakan dinding, pintu masuk / gerbang yang dikontrol, meja resepsionis berawak dan langkah-langkah lainnya. Kontrol termasuk:

* tapak perimeter dan kekuatan ditentukan oleh penilaian risiko;
* perimeter yang jelas dan ditandai, kecuali dalam situasi di mana perimeter tersembunyi / disamarkan akan meningkatkan keamanan;
* penggunaan dinding, jendela dan pintu yang sehat secara fisik, dilindungi dengan palang, kunci, alarm yang sesuai;
* penggunaan hambatan fisik tambahan, jika perlu untuk mencegah akses tidak sah atau kontaminasi fisik;
* penyediaan perlindungan yang tepat terhadap kebakaran, air, atau ancaman lingkungan yang wajar diantisipasi;
* penggunaan sistem deteksi intrusi yang tepat, seperti alarm gerak dan perimeter, pengawasan audio dan video;
* penggunaan area penerimaan berawak atau sistem kunci / ID yang sesuai untuk mengontrol jalan masuk ke area terbatas;
* langkah-langkah yang dirancang dengan redundansi yang cukup sehingga satu titik kegagalan tidak membahayakan keamanan; dan
* pemeliharaan rutin dan peninjauan kecukupan komponen perlindungan fisik ini.

Kantor, kamar, dan fasilitas yang aman • Keamanan fisik untuk kantor, kamar, dan fasilitas harus dirancang dan diimplementasikan. Kontrol termasuk:

* penggunaan tindakan yang sepadan dengan risiko yang diidentifikasi dan nilai aset yang berisiko di setiap pengaturan;
* penggunaan langkah-langkah yang menyeimbangkan kesehatan, keselamatan dan regulasi serta standar terkait;
* penggunaan kontrol yang sangat terlihat, jika sesuai sebagai pencegah;
* penggunaan kontrol / fasilitas yang tidak mencolok atau tersembunyi, jika sesuai untuk aset yang sangat sensitif; dan
* pembatasan informasi tentang fasilitas, termasuk informasi direktori dan lokasi.

Melindungi dari ancaman eksternal dan lingkungan • Perlindungan fisik terhadap kerusakan akibat kebakaran, banjir, angin, gempa bumi, ledakan, kerusuhan sipil, dan bentuk risiko alami dan buatan manusia lainnya harus dirancang dan diimplementasikan. Kontrol termasuk:

* pertimbangan kemungkinan berbagai kategori risiko dan nilai aset yang dilindungi terhadap risiko tersebut;
* pertimbangan ancaman keamanan yang ditimbulkan oleh fasilitas dan struktur tetangga;
* peralatan pemadam kebakaran yang sesuai dan tindakan pencegahan lain yang disediakan dan berlokasi di lokasi; dan
* Penentuan lokasi yang sesuai dari fasilitas cadangan dan salinan data di lokasi yang cocok di luar lokasi.

Bekerja di area yang aman • Perlindungan fisik dan pedoman untuk bekerja di area yang aman harus dirancang dan diimplementasikan. Kontrol termasuk:

* membatasi kesadaran personel tentang, dan kegiatan di dalam, lokasi yang aman berdasarkan kebutuhan-untuk-tahu;
* membatasi atau melarang pekerjaan yang tidak diawasi / tidak diawasi di tempat yang aman, baik untuk alasan keamanan maupun untuk menghindari peluang terjadinya penyimpangan;
* menjaga area aman yang kosong dikunci, tunduk pada inspeksi berkala, dan / atau dipantau dari jarak jauh yang sesuai dengan video atau teknologi lainnya;
* membatasi video, audio atau peralatan rekaman lainnya, termasuk kamera di perangkat portabel, di area yang aman.

Akses publik, akses pengiriman dan pemuatan • Jalur akses seperti area pengiriman dan pemuatan, dan titik lain di mana orang yang tidak berwenang dapat memasuki lokasi, harus dikendalikan. Kontrol termasuk:

* batas akses ke area pengiriman dan pemuatan, dan ke area akses publik lainnya, sejauh mungkin;
* inspeksi bahan yang masuk dan keluar, dan pemisahan pengiriman masuk dan keluar, jika memungkinkan; dan
* isolasi area-area ini dari fasilitas pemrosesan informasi dan area di mana informasi disimpan, jika memungkinkan.

Keamanan peralatan

Kategori ini bertujuan untuk mencegah kehilangan, kerusakan, pencurian, atau kompromi aset atau gangguan pada kegiatan organisasi.

Penempatan dan perlindungan peralatan • Peralatan harus diletakkan atau dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan untuk mengurangi peluang akses yang tidak sah oleh ancaman manusia. Kontrol termasuk:

* penempatan untuk meminimalkan risiko yang tidak perlu terhadap peralatan, dan untuk mengurangi kebutuhan akan akses tidak sah ke area sensitif;
* duduk untuk mengisolasi barang-barang yang membutuhkan perlindungan khusus, untuk meminimalkan tingkat perlindungan umum yang diperlukan;
* penggunaan kontrol partikularisasi yang sesuai untuk meminimalkan ancaman fisik - mis., pencurian atau kerusakan akibat perusakan, kebakaran, air, debu, asap, getaran, varian pasokan listrik, atau radiasi elektromagnetik; dan
* pedoman untuk makan, minum, merokok atau kegiatan lain di sekitar peralatan.

Utilitas pendukung • Peralatan harus dilindungi dari kegagalan daya, kegagalan telekomunikasi, dan gangguan lain yang disebabkan oleh kegagalan dalam utilitas pendukung seperti HVAC, pasokan air dan pembuangan limbah. Kontrol termasuk:

* memastikan bahwa utilitas pendukung memadai untuk mendukung peralatan dalam kondisi operasi normal; dan
* membuat ketentuan yang masuk akal untuk pencadangan (mis., UPS) jika terjadi kegagalan utilitas pendukung.

Keamanan kabel • Kabel daya dan telekomunikasi yang membawa data sensitif atau layanan informasi pendukung harus dilindungi dari intersepsi atau kerusakan. Kontrol termasuk:

* langkah-langkah fisik untuk mencegah intersepsi atau kerusakan yang tidak sah, termasuk perlindungan tambahan untuk sistem sensitif atau kritis;
* perutean alternatif / cadangan atau media transmisi jika diperlukan, khususnya untuk sistem kritis;
* tanda kabel dan peralatan yang diidentifikasi dengan jelas, kecuali jika keamanan ditingkatkan dengan menghapus / menyembunyikan tanda tersebut; dan
* dokumentasi tambalan dan kegiatan perawatan lainnya.

Pemeliharaan peralatan • Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan. Kontrol termasuk:

* pemeliharaan preventif yang tepat;
* dokumentasi semua kegiatan pemeliharaan, termasuk pemeliharaan preventif terjadwal;
* dokumentasi semua dugaan atau kesalahan aktual, dan remediasi terkait;
* pemeliharaan hanya oleh karyawan yang berwenang atau pihak ketiga yang dikontrak; dan
* langkah-langkah keamanan yang tepat, seperti pembersihan informasi atau pengawasan proses perawatan, sesuai dengan sensitivitas informasi pada atau dapat diakses oleh perangkat yang dipelihara;

Keamanan peralatan di luar lokasi • Langkah-langkah keamanan yang tepat harus diterapkan pada peralatan di luar lokasi, dengan mempertimbangkan risiko yang berbeda dari bekerja di luar lokasi organisasi. Kontrol termasuk:

* otorisasi dari setiap pemrosesan informasi organisasi di luar lokasi, terlepas dari kepemilikan perangkat pengolah;
* kontrol keamanan untuk peralatan dalam perjalanan dan di luar lokasi, sesuai dengan pengaturan dan sensitivitas informasi pada atau dapat diakses oleh perangkat;
* perlindungan asuransi yang memadai, di mana asuransi pihak ketiga hemat biaya; dan
* kesadaran karyawan dan kontraktor akan tanggung jawab mereka untuk melindungi informasi dan perangkat itu sendiri, dan risiko tertentu dari lingkungan di luar lokasi.

Pembuangan atau penggunaan kembali peralatan yang aman • Semua peralatan yang mengandung media penyimpanan harus diperiksa untuk memastikan bahwa data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa dengan aman sebelum dibuang. Kontrol termasuk:

* penggunaan metode yang diterima secara umum untuk menghapus informasi yang aman, sesuai dengan sensitivitas informasi yang diketahui atau diyakini ada di media;
* penghapusan informasi yang aman oleh personel yang terlatih secara tepat, atau verifikasi penghapusan informasi yang aman oleh personel yang terlatih dengan tepat.

Penghapusan properti • Peralatan, informasi atau perangkat lunak tidak boleh diambil di luar lokasi tanpa izin sebelumnya. Kontrol termasuk:

* pembatasan pada jenis / jumlah informasi atau peralatan yang dapat diambil di luar lokasi;
* rekaman otorisasi di luar lokasi dan inventaris peralatan dan informasi yang diambil di luar lokasi; dan
* bagi orang yang berwenang untuk membawa peralatan atau informasi di luar lokasi, kesadaran yang tepat akan risiko keamanan yang terkait dengan lingkungan di luar lokasi dan pelatihan dalam kontrol dan tindakan balasan yang sesuai.
1. **Communications and Operations Management (Manajemen Komunikasi dan Operasi)**

Control ini bertujuan utama untuk mengurangi risiko kegagalan serta konsekuensi finansial maupun teknis dengan memastikan bahwa semua tool pengolahan data dan informasi perusahaan (printer, PC, dan sebagainya) telah digunakan sebagaimana mestinya dan berdasarkan kaidah-kaidah keamanan informasi.

1. **Access Control (kontrol akses)**

Control ini mengatur serta mengelola bagaimana seharusnya akses terhadap data dan informasi perusahaan dilakukan oleh staf/karyawan maupun pihak-pihak eksternal perusahaan. Beberapa bentuk dari control ini di antaranya adalah penerapan mekanisme otorisasi sistem seperti kebijakan penggunaan password untuk mengakses sistem jaringan perusahaan untuk penggunaan aplikasi, e-mail, dan sebagainya.

Kontrol akses biasanya dianggap sebagai kegiatan teknis yang berkaitan dengan pembukaan akun, pengaturan kata sandi, dan hal-hal serupa - dan memang benar: kontrol akses memang mencakup semua hal ini, tetapi kontrol akses tidak dimulai sebagai hal teknis. Ini dimulai sebagai keputusan bisnis.

Mari kita lihat apa yang disyaratkan ISO 27001: ia mendefinisikan kontrol akses di bagian A.9 dari Lampiran A, total 14 kontrol (ditempatkan di 4 subbagian) - lebih dari 12% dari semua kontrol dalam standar ini - yang berarti topik ini jelas sangat penting. Mari kita lihat seperti apa kontrol ini.

Persyaratan bisnis kontrol akses

Subbagian ini mengharuskan Anda untuk menetapkan Kebijakan Kontrol Akses, dan untuk menentukan pengguna mana yang akan memiliki akses ke jaringan dan layanan mana. Akibatnya, ini berarti Anda harus menetapkan aturan terlebih dahulu, dan hanya kemudian memungkinkan pengguna untuk menelusuri jaringan dan layanan Anda.

Anda dapat mengatur aturan akses dengan beberapa cara, tetapi biasanya ada dua pendekatan: pendekatan pertama adalah Anda mendefinisikan profil pengguna (di mana Anda menentukan tingkat akses untuk setiap profil pengguna), dan kemudian berdasarkan pada setiap jabatan yang Anda tetapkan. profil pengguna yang sesuai dengan jabatan itu. Misalnya, Anda dapat menetapkan bahwa Anda memiliki profil pengguna A (dengan akses ke aplikasi dan layanan dasar), dan profil pengguna B (dengan akses ke semua sistem dasar + yang lebih sensitif) - maka Anda dapat menetapkan aturan di mana setiap orang di perusahaan menggunakan profil pengguna A, sementara hanya beberapa pengguna istimewa (mis., administrator, manajer, dll.) menggunakan profil pengguna B.

Pendekatan kedua adalah Anda mendefinisikan bahwa pemilik aset (yaitu, jaringan, aplikasi, layanan, dll.) Harus menyetujui akses ke pengguna tertentu setiap kali mereka perlu mengakses aset tersebut - pendekatan kedua ini, tentu saja, jauh lebih membuang-buang waktu. Pada kenyataannya, kombinasi dari dua pendekatan ini sangat sering digunakan, seperti yang akan saya jelaskan nanti.

Omong-omong, Kebijakan Kontrol Akses hanya dapat fokus pada sistem informasi, atau keduanya pada sistem informasi dan akses fisik ke area yang aman - standar memungkinkan kedua pendekatan. Pada kenyataannya, menyetujui akses ke area fisik tidak memiliki terlalu banyak perbedaan dibandingkan dengan menyetujui akses ke sistem informasi.

Manajemen akses pengguna

Di sinilah hal-hal mulai menjadi teknis - Anda harus menentukan bagaimana Anda mengharuskan pengguna untuk mendaftar di sistem Anda (misalnya, menangani ID pengguna), bagaimana Anda menetapkan mereka akses (penyediaan akses atau mencabut akses), dan bagaimana Anda mengelola data otentikasi (mis., bagaimana Anda memberikan kata sandi awal, kartu pintar, dll.).

Tetapi sekali lagi, Anda harus mengurus beberapa hal organisasi - misalnya, jika Anda harus mengizinkan akses yang di luar aturan reguler (akses istimewa), Anda perlu menentukan dengan tepat siapa yang dapat menyetujui pengecualian akses pengguna tersebut. Apa yang biasanya dilakukan adalah perusahaan menentukan profil pengguna, dan jika ada akses yang harus disetujui di atas itu, ini diperlakukan sebagai akses istimewa dan kemudian pemilik aset harus menyetujui pengecualian tersebut.

Karena pengecualian seperti itu akan selalu ada, pemilik aset harus secara teratur meninjau semua akses istimewa dan memutuskan apakah masih diperlukan - sangat sering Anda akan mengalami situasi di mana akses istimewa disetujui sejak lama, hanya untuk mengetahuinya ada kemungkinan. risiko keamanan tinggi dan tidak ada kebutuhan operasional untuk akses tersebut.

Akhirnya, harus ada proses penghapusan semua hak akses ketika seseorang meninggalkan perusahaan atau menyesuaikannya ketika seseorang mengubah posisi mereka di perusahaan. Sudah terlalu sering terjadi bahwa orang memiliki akses ke beberapa sistem beberapa tahun setelah mereka meninggalkan perusahaan, hanya karena tidak ada yang ingat untuk menutup akses ini.

Omong-omong, Anda dapat menetapkan semua aturan itu dalam Kebijakan Kontrol Akses yang sama, atau Anda dapat mengembangkan dokumen terpisah untuk tujuan itu - misalnya, Anda mungkin mengembangkan Kebijakan Kata Sandi tempat Anda mendefinisikan cara melakukan otentikasi.

Tanggung jawab pengguna

Ini adalah subbagian yang sangat singkat (dengan satu kontrol saja) yang mengharuskan Anda menentukan bagaimana pengguna akan merahasiakan informasi otentikasi mereka (mis., Melindungi kata sandi mereka). Ini biasanya dilakukan melalui beberapa dokumen seperti Kebijakan Penggunaan yang Dapat Diterima, yang menetapkan aturan seperti ini: jangan tulis kata sandi, jangan ungkapkan kepada siapa pun, jangan gunakan kata sandi yang sama di sistem yang berbeda, dll.

Kontrol akses sistem dan aplikasi

Di sinilah segalanya menjadi lebih teknis - Anda harus memastikan bahwa akses ke semua sistem benar-benar sesuai dengan Kebijakan Kontrol Akses, bahwa akses dilindungi dengan prosedur masuk log yang aman (misalnya, gunakan biometrik jika kata sandi tidak cukup) , kata sandi yang digunakan cukup kompleks dan cukup aman, dll.

Lebih lanjut, jika perusahaan Anda sedang mengembangkan program, Anda harus menentukan bagaimana melindungi akses ke kode sumber - biasanya, akses didefinisikan melalui Kebijakan Kontrol Akses yang sama dengan semua masalah akses lainnya.

Terakhir, Anda harus menentukan cara melindungi akses ke informasi saat menggunakan alat perangkat lunak khusus yang memungkinkan akses ke informasi secara langsung, melewati aplikasi standar atau kontrol sistem - ini biasanya administrator dan program utilitas, terutama digunakan oleh administrator sistem. Dalam kasus apa pun, penggunaan alat tersebut harus dibatasi, diizinkan untuk digunakan hanya dalam keadaan yang sangat spesifik, dan di bawah pengawasan.

Untuk menyimpulkan, tidak memiliki kontrol akses berarti tidak memiliki keamanan sama sekali - ini adalah salah satu blok bangunan utama keamanan informasi yang harus dilakukan secara teknis dengan baik, tetapi juga dirancang sedemikian rupa sehingga cukup aman dan dapat diterima oleh pengguna. Apa yang tidak Anda inginkan terjadi adalah memiliki rencana yang sangat ambisius untuk mengubah kata sandi setiap bulan, hanya untuk mengetahui bahwa karyawan Anda telah sepenuhnya menolak sistem seperti itu karena mereka pikir itu tidak praktis.

1. **Information System Acquisition, Development, and Maintenance (Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi)**

Control ini bertujuan untuk mencegah modifikasi serta penyalahgunaan informasi yang terdapat di dalam operating system (PC yang digunakan oleh user) maupun dalam aplikasi.

Analisis & Spesifikasi Persyaratan Keamanan Informasi

Persyaratan terkait keamanan informasi perlu dimasukkan dalam persyaratan apa pun untuk sistem informasi baru atau peningkatan pada sistem informasi yang ada. Ini dapat terjadi bersamaan dengan A.6.1.5 sebagai bagian dari keamanan informasi dalam proyek-proyek dan harus memperhitungkan nilai informasi yang berisiko yang dapat diselaraskan dengan skema klasifikasi informasi dalam A.8.2.1.

Dalam setiap pengembangan sistem baru atau perubahan ke sistem yang ada, penting untuk memahami apa persyaratan bisnis untuk kontrol keamanan dengan melakukan penilaian risiko. Ini harus dilakukan sebelum pemilihan atau dimulainya pengembangan solusi. Pertimbangan keamanan harus terjadi dari peluang sedini mungkin untuk memastikan bahwa persyaratan yang benar diidentifikasi sebelum pemilihan solusi dimulai. Persyaratan keamanan harus didokumentasikan dan disepakati sehingga mereka dapat dirujuk ketika solusinya diperoleh atau dikembangkan. Ini bukan praktik yang baik untuk memilih atau mengembangkan solusi dan kemudian menilai tingkat kemampuan keamanan sesudahnya. Ini sering mengarah pada risiko dan biaya yang lebih tinggi dan juga dapat menyebabkan masalah dalam undang-undang yang berlaku seperti GDPR yang mendorong keamanan dengan filosofi desain dan teknik seperti Penilaian Dampak Privasi Perlindungan Data (DPIA). Ada juga banyak situs web yang mendukung praktik pengembangan yang aman dan prinsip-prinsip utama untuk dipertimbangkan seperti yang dianjurkan oleh National Cyber ​​Security Center (NCSC). ISO 27002 juga termasuk panduan implementasi. Prinsip mana pun yang diikuti harus didokumentasikan.

Auditor akan mencari untuk melihat bahwa keamanan sedang dipertimbangkan pada semua tahap siklus hidup proyek, untuk sistem baru atau perubahan ke sistem yang ada. Mereka juga akan berharap untuk melihat pertimbangan untuk kerahasiaan, integritas dan ketersediaan minimal sebelum proses seleksi atau pengembangan dimulai.

Mengamankan Layanan Aplikasi di Jaringan Publik

Informasi yang terlibat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari aktivitas penipuan, sengketa kontrak dan pengungkapan dan modifikasi yang tidak sah. Untuk layanan yang disediakan melalui jaringan publik, seperti internet, penting untuk memahami tingkat risiko yang terlibat dan persyaratan bisnis untuk melindungi informasi. Sekali lagi, penting untuk mempertimbangkan kerahasiaan, integritas, dan ketersediaan.

Ketika transaksi keuangan atau informasi pribadi yang sensitif merupakan bagian dari layanan, sangat penting untuk mempertimbangkan keamanan untuk meminimalkan risiko aktivitas penipuan di mana persyaratan GDPR untuk enkripsi dan perlindungan lainnya harus menjadi persyaratan minimum. Setelah beroperasi, penting untuk memastikan bahwa layanan seperti itu terus-menerus dipantau untuk serangan atau aktivitas yang tidak diinginkan. Auditor akan berharap untuk melihat pertimbangan untuk layanan aplikasi "seberapa aman" melalui jaringan publik perlu, dengan keputusan berdasarkan penilaian risiko dan persyaratan hukum, peraturan dan kontrak lainnya.

Melindungi Transaksi Layanan Aplikasi

Informasi yang terlibat dalam transaksi layanan aplikasi harus dilindungi untuk mencegah pengiriman yang tidak lengkap, kesalahan rute, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi atau pengulangan pesan yang tidak sah. Perlindungan tambahan kemungkinan akan mengamankan transaksi layanan aplikasi (tidak harus hanya transaksi keuangan). Ini mungkin termasuk; Penggunaan tanda tangan elektronik, Penggunaan enkripsi; dan Penggunaan protokol aman. Pemantauan yang berkelanjutan atas transaksi-transaksi semacam itu sedekat mungkin dengan waktu nyata juga diperlukan.

Kebijakan Pengembangan yang Aman

Aturan untuk pengembangan perangkat lunak dan sistem harus ditetapkan dan diterapkan pada pengembangan dalam organisasi. Kebijakan pengembangan yang aman digunakan untuk memastikan bahwa lingkungan pengembangan itu sendiri aman dan bahwa proses untuk mengembangkan dan menerapkan perubahan sistem dan sistem mendorong penggunaan pengkodean yang aman dan praktik pengembangan. Kebijakan tersebut akan mencakup menunjukkan bagaimana keamanan perlu dipertimbangkan pada semua tahap siklus hidup pengembangan mulai dari desain hingga implementasi langsung. Bahasa pengkodean khusus dan alat pengembangan memiliki kerentanan yang berbeda dan memerlukan teknik “pengerasan” yang berbeda sesuai dan penting bahwa ini diidentifikasi dan disepakati dan pengembang dibuat sadar akan tanggung jawab mereka untuk mengikutinya. Kebijakan yang patuh akan membahas pos pemeriksaan keamanan selama pengembangan; repositori aman; keamanan dalam kontrol versi; pengetahuan keamanan aplikasi; dan kemampuan pengembang untuk menghindari kerentanan, lalu menemukan dan memperbaikinya ketika terjadi.

Auditor akan mencari di sini untuk melihat bahwa pertimbangan keamanan sesuai dengan tingkat risiko untuk sistem yang sedang dikembangkan atau diubah dan bahwa mereka yang melakukan pengembangan memahami perlunya memasukkan pertimbangan keamanan di seluruh siklus hidup pengembangan. Penapisan awal yang kuat dalam mempekerjakan keterampilan ini, manajemen inlife dan pelatihan sumber daya sangat penting dan praktik seperti pemrograman pasangan, ulasan sejawat dan jaminan kualitas independen, tinjauan kode dan pengujian adalah atribut positif.

Prosedur Kontrol Perubahan Sistem

Perubahan pada sistem dalam siklus pengembangan harus dikontrol dengan menggunakan prosedur kontrol perubahan formal. Prosedur kontrol perubahan sistem harus diintegrasikan dengan, diselaraskan dan mendukung kontrol perubahan operasional. Prosedur manajemen perubahan formal dirancang untuk mengurangi risiko pengembangan kerentanan yang disengaja atau tidak disengaja yang dapat memungkinkan sistem dikompromikan begitu perubahan tersebut diberlakukan. Untuk kontrol perubahan sistem, penting bagi pemilik sistem untuk memahami perubahan apa yang dilakukan pada sistem mereka, mengapa dan oleh siapa. Adalah tanggung jawab mereka untuk memastikan bahwa sistem mereka tidak dikompromikan melalui pengembangan yang buruk atau jahat. Karena itu mereka harus dilibatkan dalam menetapkan aturan untuk otorisasi dan pengujian dan pengecekan pra-live. Catatan audit diperlukan untuk memberikan bukti penggunaan prosedur perubahan yang benar. ISO 27002 mendokumentasikan banyak aspek pengendalian perubahan yang harus dimasukkan, mulai dari dokumentasi sederhana perubahan hingga pertimbangan waktu penyebaran untuk menghindari dampak bisnis yang negatif. Kontrol ini seperti yang lainnya di A.14 juga selaras dengan prosedur yang didokumentasikan dalam A.12.1.2.

Tinjauan Teknis Aplikasi Setelah Perubahan Platform Pengoperasian

Ketika platform operasi diubah, aplikasi penting bisnis perlu ditinjau dan diuji untuk memastikan tidak ada dampak buruk pada operasi atau keamanan organisasi. Ketika platform sistem operasi diubah, adalah hal biasa bahwa beberapa aplikasi mungkin memiliki masalah kompatibilitas. Oleh karena itu penting untuk menguji perubahan sistem operasi dalam pengembangan atau lingkungan pengujian di mana aplikasi bisnis penting dapat diperiksa untuk kompatibilitas dengan OS yang diubah. Prosedur untuk kontrol dan pengujian perubahan sistem operasi harus mengikuti kontrol manajemen perubahan standar.

Batasan tentang Perubahan pada Paket Perangkat Lunak

Modifikasi pada paket perangkat lunak perlu dicegah, terbatas pada perubahan yang diperlukan dan semua perubahan harus dikontrol dengan ketat. Paket perangkat lunak yang disediakan vendor dirancang untuk pasar massal dan tidak benar-benar dirancang untuk organisasi yang membuat perubahan sendiri. Bahkan sebagian besar waktu kemampuan untuk membuat perubahan seperti itu dikunci oleh vendor dan kustomisasi terbatas dalam paket. Ketika perangkat lunak open-source digunakan, jauh lebih mungkin bahwa perubahan dapat dibuat oleh organisasi, namun, ini harus dibatasi dan dikendalikan untuk memastikan bahwa perubahan yang dilakukan tidak memiliki dampak buruk pada integritas internal atau keamanan perusahaan. perangkat lunak.

Prinsip-prinsip Teknik Sistem Aman

Prinsip-prinsip untuk sistem keamanan rekayasa harus ditetapkan, didokumentasikan, dipelihara, dan diterapkan pada setiap upaya implementasi sistem informasi. Prinsip-prinsip rekayasa perangkat lunak yang aman ada di tingkat umum dan khusus untuk platform pengembangan dan bahasa pengkodean. Di mana pun pengembangan dilakukan, pertimbangan untuk pemilihan dan penerapan prinsip-prinsip tersebut harus dipertimbangkan, dinilai, didokumentasikan secara formal dan diamanatkan. Auditor akan ingin melihat bahwa seperti halnya dengan banyak kontrol, penggunaan prinsip-prinsip rekayasa sistem dipertimbangkan terhadap tingkat risiko yang diidentifikasi dan akan mencari bukti untuk mendukung pilihan yang dibuat.

Lingkungan Pengembangan yang Aman

Organisasi perlu membangun dan melindungi lingkungan pengembangan yang aman untuk pengembangan sistem dan upaya integrasi yang mencakup seluruh siklus pengembangan sistem. Lingkungan pengembangan perlu dilindungi untuk memastikan pengembangan berbahaya dan tidak disengaja serta pembaruan kode yang dapat menciptakan kerentanan atau kompromi kerahasiaan, integritas, dan ketersediaan. Persyaratan perlindungan harus ditentukan dari penilaian risiko, persyaratan bisnis dan persyaratan internal dan eksternal lainnya termasuk undang-undang, peraturan, perjanjian atau kebijakan kontrak. Secara khusus, jika segala bentuk data langsung digunakan dalam lingkungan pengembangan, ia perlu dilindungi dan dikontrol secara khusus.

Pengembangan Outsourced

Organisasi harus mengawasi dan memantau aktivitas pengembangan sistem outsourcing. Jika pengembangan sistem dan perangkat lunak dialihdayakan baik seluruhnya atau sebagian kepada pihak eksternal, persyaratan keamanan harus ditentukan dalam kontrak atau perjanjian terlampir. Di sinilah Lampiran A 15.1 penting untuk memiliki yang benar serta A.13.2.4 untuk pengungkapan rahasia dan kerahasiaan.

Penting juga untuk mengawasi dan memantau pengembangan untuk mendapatkan kepastian bahwa standar dan persyaratan organisasi untuk keamanan dalam sistem tercapai. Bergantung pada bagaimana mitra outsourcing tertanam di dalam organisasi, terutama jika staf berada di lokasi organisasi, penting untuk memasukkan staf mereka dalam pelatihan kesadaran keamanan dan program-program kesadaran dan komunikasi. Sangat penting untuk memastikan bahwa praktik keamanan internal dari mitra outsourcing, mis. pemeriksaan staf, setidaknya memenuhi persyaratan jaminan yang relevan dengan tingkat risiko terkait dengan perkembangan yang akan mereka kerjakan.

Auditor akan mencari untuk melihat di mana outsourcing digunakan, ada bukti uji tuntas sebelum, selama dan setelah keterlibatan mitra outsourcing telah dilakukan dan termasuk pertimbangan untuk ketentuan keamanan informasi.

Pengujian Keamanan Sistem

Pengujian fungsionalitas keamanan perlu dilakukan selama pengembangan. Pengujian khusus terhadap fungsionalitas keamanan untuk pengembangan apa pun harus dilakukan dan ditandatangani oleh otoritas yang sesuai dengan kompetensi dan tanggung jawab keamanan. Pengujian keamanan hasil yang diharapkan harus didokumentasikan sebelum pengujian dimulai dan harus didasarkan pada persyaratan bisnis untuk keamanan. Auditor akan ingin melihat bahwa ada bukti bahwa pengujian khusus keamanan telah dilakukan dalam setiap pengembangan yang relevan dengan keamanan.

Pengujian Penerimaan Sistem

Program pengujian penerimaan dan kriteria terkait harus ditetapkan untuk sistem informasi baru, peningkatan dan versi baru. Untuk pengujian penerimaan, pengujian dan kriteria untuk menunjukkan pengujian yang berhasil harus dirancang dan dikembangkan berdasarkan persyaratan bisnis sebelum pengujian dilakukan. Pengujian penerimaan juga harus mencakup pengujian keamanan. Auditor akan mencari bukti yang menunjukkan kriteria dan metode pengujian penerimaan dirancang sesuai dengan persyaratan bisnis dan termasuk ketentuan untuk pengujian penerimaan keamanan.

1. **Information Security Incident Management (Manajemen Insiden Keamanan Informasi)**

Control ini terdiri dari beberapa aspek sebagai berikut:

– Adanya proses pelaporan yang sesuai jika terjadi peristiwa seperti bocornya data dan informasi rahasia perusahaan ke tangan pihak-pihak yang tidak berwenang.
– Adanya proses maupun prosedur yang dapat memastikan bahwa sebuah kejadian keamanan (security incident) tidak terjadi lagi di kemudian hari dengan mengetahui apa penyebabnya serta proses pencarian solusi permanen yang memadai.

Tanggung Jawab & Prosedur

Kontrol yang baik menggambarkan bagaimana manajemen menetapkan tanggung jawab dan prosedur untuk memastikan respons yang cepat, efektif, dan teratur untuk mengatasi kelemahan, peristiwa, dan insiden keamanan. Dalam istilah yang sederhana, sebuah insiden adalah di mana beberapa bentuk kerugian telah terjadi seputar kerahasiaan, integritas, atau ketersediaan. Contohnya adalah di mana jendela dibiarkan terbuka dan pencuri mencuri file penting yang duduk di atas meja ....... Mengikuti utas itu, suatu peristiwa adalah di mana jendela dibiarkan terbuka tetapi tidak ada yang mencuri file itu. Kelemahannya adalah bahwa jendela mudah pecah atau tua dan bisa menjadi tempat yang jelas untuk pembobolan. Kelemahan juga merupakan manajemen risiko umum atau peluang peningkatan.

Prosedur untuk insiden, kejadian, dan perencanaan respons kelemahan perlu didefinisikan secara jelas sebelum insiden terjadi dan disetujui oleh pimpinan Anda. Prosedur-prosedur itu cukup mudah untuk dikembangkan karena sisa dari kendali Annex A ini menjabarkannya. Auditor Anda akan berharap untuk melihat semua prosedur formal dan terdokumentasi ini di tempat, dan bukti bahwa mereka berfungsi.

Melaporkan Kejadian Keamanan Informasi

Kontrol yang baik di sini memastikan bahwa insiden dan peristiwa keamanan informasi dapat dilaporkan melalui saluran manajemen yang sesuai sesegera mungkin.

Karyawan dan pihak berkepentingan terkait (mis. Pemasok) perlu diberi tahu tentang kewajiban mereka untuk melaporkan insiden keamanan dan Anda harus menutupinya sebagai bagian dari kesadaran dan pelatihan umum Anda. Untuk melakukan ini dengan baik, mereka perlu memiliki kesadaran tentang apa yang merupakan kelemahan, peristiwa atau insiden keamanan informasi, jadi jelaslah tentang itu, berdasarkan contoh sederhana di atas. Jika suatu peristiwa keamanan informasi terjadi atau diduga telah terjadi, itu harus segera dilaporkan kepada administrator keamanan informasi yang ditunjuk dan yang perlu didokumentasikan sesuai dengan itu.

Beberapa kemungkinan alasan untuk melaporkan insiden keamanan meliputi; kontrol keamanan yang tidak efektif; dugaan pelanggaran integritas atau kerahasiaan informasi, atau masalah ketersediaan mis. tidak dapat mengakses layanan.

Auditor akan ingin melihat dan akan mengambil sampel untuk bukti kesadaran tentang apa yang merupakan kelemahan, peristiwa atau kejadian di antara staf umum, dan kesadaran akan prosedur dan tanggung jawab pelaporan insiden.

Melemah Kelemahan Keamanan Informasi

Kontrol ini hanya didasarkan pada insiden dan peristiwa tetapi mungkin diperlakukan sedikit berbeda setelah dilaporkan (lihat A.16.1.4)

Penting bagi karyawan untuk menyadari fakta bahwa ketika menemukan kelemahan keamanan, mereka tidak boleh berusaha membuktikan kelemahan itu, karena pengujian dapat diartikan sebagai penyalahgunaan sistem, sementara juga berisiko merusak sistem dan informasi yang tersimpan. , menyebabkan insiden keamanan!

Penilaian & Keputusan tentang Kejadian Keamanan Informasi

Kejadian keamanan informasi harus dinilai dan kemudian dapat diputuskan jika harus diklasifikasikan sebagai insiden keamanan informasi, peristiwa kelemahan. Setelah peristiwa keamanan dilaporkan dan kemudian dicatat, maka perlu dinilai untuk menentukan tindakan terbaik yang harus diambil. Tindakan ini harus bertujuan untuk meminimalkan kompromi dari ketersediaan, integritas, atau kerahasiaan informasi dan mencegah insiden lebih lanjut. Idealnya itu akan berdampak minimal bagi pengguna layanan lainnya. Pertimbangan tentang siapa yang perlu diberitahu tentang kejadian tersebut, secara internal, pelanggan, pemasok, regulator dapat terjadi di bagian siklus hidup ini juga.

GDPR dan Undang-Undang Perlindungan Data 2018 berarti bahwa beberapa insiden keamanan informasi yang berkaitan dengan data pribadi juga harus dilaporkan ke Otoritas Pengawas, sehingga kontrol Anda juga harus mengikat dalam pertimbangan ini untuk memenuhi persyaratan peraturan dan menghindari duplikasi atau kesenjangan dalam pekerjaan.

Respon terhadap Insiden Keamanan Informasi

Itu selalu baik untuk menetapkan pemilik, memperjelas tindakan dan rentang waktu, dan seperti segala sesuatu untuk ISO 27001, simpan informasi untuk tujuan audit (juga penting jika Anda memiliki pemangku kepentingan dan regulator lain untuk dipertimbangkan). Individu yang ditugaskan menangani peristiwa keamanan akan bertanggung jawab untuk memulihkan tingkat keamanan normal sementara juga;

* mengumpulkan bukti sesegera mungkin setelah kejadian;
* melakukan analisis forensik keamanan informasi (istilah besar tetapi setidaknya menjadi jelas tentang akar permasalahan dan aspek terkait atau apa yang terjadi dan siapa yang terlibat, mengapa dll);
* eskalasi, jika diperlukan, misalnya ke regulator yang relevan;
* memastikan bahwa semua kegiatan respons yang terlibat dicatat dengan benar untuk analisis nanti;
* mengomunikasikan keberadaan insiden keamanan informasi atau perincian yang relevan kepada pimpinan agar mereka dapat dikomunikasikan lebih lanjut kepada berbagai individu atau organisasi berdasarkan kebutuhan yang perlu diketahui; dan
* berurusan dengan kelemahan keamanan informasi yang ditemukan menyebabkan atau berkontribusi pada insiden tersebut.

Belajar dari Insiden Keamanan Informasi

Ini adalah kontrol penting, dan kebijakan Anda perlu menunjukkan bahwa pengetahuan yang diperoleh dari menganalisis dan menyelesaikan insiden keamanan informasi akan digunakan untuk membantu mengurangi kemungkinan atau dampak dari setiap insiden di masa depan.

Sebagai bagian dari komitmen untuk peningkatan layanan berkelanjutan, Anda harus memastikan bahwa Anda belajar dari pelajaran dari setiap insiden keamanan untuk membantu mengembangkan dan mengadaptasi ISMS untuk memenuhi lanskap yang berubah yang bekerja di dalamnya.

Setelah insiden telah diselesaikan, itu harus ditempatkan ke dalam status tinjauan dan pembelajaran, di mana responden utama untuk insiden itu akan membahas setiap perubahan yang diperlukan untuk proses kebijakan SMKI sebagai hasilnya. Setiap rekomendasi yang relevan harus diajukan kepada Dewan ISMS untuk diskusi lebih lanjut.

Setelah peninjauan dan pembelajaran telah selesai, pembaruan telah dibuat untuk kebijakan yang diperlukan, staf yang relevan harus diberitahu dan dilatih kembali jika diperlukan, dan siklus kesadaran keamanan informasi dan pendidikan terus berlanjut.

Pengumpulan Bukti

Organisasi harus menetapkan dan menerapkan kontrol untuk identifikasi, pengumpulan, perolehan, dan pelestarian informasi, yang dapat digunakan sebagai bukti, terutama jika ada proses pidana atau perdata yang kemungkinan terjadi akibat insiden tersebut.

Jika organisasi mencurigai atau mengetahui bahwa insiden keamanan dapat mengakibatkan tindakan hukum atau disipliner, mereka harus melakukan pengumpulan bukti dengan hati-hati, memastikan rantai penahanan yang baik dan menghindari ancaman tertangkap oleh manajemen yang buruk.

Masuk akal untuk mengikat manajemen insiden keamanan informasi dengan jelas dengan prosedur disiplin juga. Setiap orang harus tahu untuk mengambil tindakan pencegahan sementara juga menjadi jelas tentang konsekuensi bagi mereka yang gagal untuk menganggapnya serius.

1. **Business Continuity Management (Manajemen Kontinuitas Bisnis)**

Control ini memastikan bahwa perusahaan memiliki kemampuan untuk bereaksi secara cepat terhadap kemungkinan terjadinya gangguan pada berjalannya proses bisnis yang kritikal dari kegagalan sistem aplikasi, bencana alam, dan lain sebagainya.

Merencanakan Kesinambungan Keamanan Informasi

Organisasi harus menentukan persyaratannya untuk keamanan informasi dan kelangsungan manajemen keamanan informasi dalam situasi yang merugikan, mis. saat krisis atau bencana. ISMS terbaik akan memiliki kontrol Annex A yang lebih luas yang memitigasi terhadap kebutuhan untuk mengimplementasikan proses pemulihan bencana atau rencana kesinambungan bisnis sejalan dengan A.17. Meskipun demikian, insiden gangguan yang lebih signifikan mungkin masih terjadi sehingga perencanaan untuk mereka penting. Apa yang terjadi ketika pusat data utama dengan informasi dan aplikasi Anda di dalamnya menjadi tidak tersedia? Apa yang terjadi ketika pelanggaran data besar terjadi, serangan ransomware dilakukan atau orang kunci dalam bisnis tidak beroperasi, atau mungkin Kantor Pusat mengalami banjir besar …… ..?

Setelah mempertimbangkan berbagai peristiwa dan skenario yang perlu direncanakan, organisasi kemudian dapat mendokumentasikan rencana tersebut dengan rincian apa pun yang diperlukan untuk menunjukkannya memahami masalah tersebut dan langkah-langkah yang diperlukan untuk mengatasinya.

ISO 22301 menawarkan pendekatan yang lebih terstruktur untuk kesinambungan bisnis yang sangat pas dengan persyaratan utama ISO 27001.

Menerapkan Kesinambungan Keamanan Informasi

Rumah sakit perlu menetapkan, mendokumentasikan, menerapkan, dan memelihara proses, prosedur, dan kontrol untuk memastikan tingkat kontinuitas yang diperlukan untuk keamanan informasi selama situasi yang mengganggu. Setelah persyaratan diidentifikasi, organisasi harus menerapkan kebijakan, prosedur, dan kontrol fisik atau teknis lainnya yang memadai dan proporsional untuk memenuhi persyaratan tersebut. Uraian tentang tanggung jawab, kegiatan, pemilik, rentang waktu, mitigasi pekerjaan yang harus dilakukan (di luar risiko dan kebijakan yang sudah beroperasi misalnya komunikasi krisis). Struktur manajemen dan titik pemicu eskalasi yang relevan harus diidentifikasi untuk memastikan bahwa jika dan ketika suatu peristiwa bertambah parah, eskalasi yang relevan ke otoritas yang sesuai dibuat secara efektif dan tepat waktu. Ini juga harus dibuat jelas ketika ada pengembalian ke bisnis seperti biasa dan setiap proses BCP berhenti.

Memverifikasi, Meninjau & Mengevaluasi Kelanjutan Keamanan Informasi

Organisasi harus memverifikasi kontrol kontinuitas keamanan informasi yang ditetapkan dan diterapkan secara berkala untuk memastikan bahwa mereka valid dan efektif selama situasi ini. Kontrol yang diterapkan untuk kontinuitas keamanan informasi harus diuji, ditinjau, dan dievaluasi secara berkala untuk memastikan kontrol terhadap perubahan dalam bisnis, teknologi, dan tingkat risiko. Auditor akan ingin melihat bahwa ada bukti; Pengujian berkala atas rencana dan kontrol; Catatan doa rencana dan tindakan yang diambil untuk resolusi dan pelajaran yang dipetik; dan Tinjauan berkala dan manajemen perubahan untuk memastikan bahwa rencana dipertahankan terhadap perubahan.

1. **Compliance (Kepatuhan)**

Control ini memastikan bahwa semua peraturan pemerintah atau negara yang berlaku di tempat domisili perusahaan telah dipatuhi dan bahwa semua kebijakan keamanan informasi telah mengacu pada peraturan-peraturan tersebut. Contohnya mudah ditemui di industri perbankan, misalnya dengan kebijakan anti-money laundering atau pencucian uang, dimana perbankan harus mewajibkan semua nasabahnya membuat pernyataan terkait dari mana mereka memperoleh dana tersebut.

Identifikasi Perundang-undangan yang Berlaku & Persyaratan Kontrak

Kontrol yang baik menjelaskan bagaimana semua undang-undang, peraturan, persyaratan kontrak, dan pendekatan organisasi yang relevan untuk memenuhi persyaratan ini harus secara eksplisit diidentifikasi, didokumentasikan, dan selalu diperbarui untuk setiap sistem informasi dan organisasi. Sederhananya, organisasi perlu memastikan bahwa organisasi ini selalu mengikuti dan mendokumentasikan undang-undang dan peraturan yang memengaruhi pencapaian tujuan bisnisnya dan hasil dari SMKI.

Adalah penting bahwa organisasi memahami peraturan, peraturan, dan persyaratan kontrak yang harus dipatuhi dan ini harus dicatat secara terpusat dalam daftar untuk memungkinkan kemudahan manajemen dan koordinasi. Identifikasi apa yang relevan akan sangat tergantung pada; Di mana organisasi berada atau beroperasi; Apa sifat bisnis organisasi itu; dan Sifat informasi yang ditangani dalam organisasi. Identifikasi undang-undang yang relevan, peraturan dan persyaratan kontrak kemungkinan akan mencakup keterlibatan dengan para ahli hukum, badan pengatur dan manajer kontrak.

Ini adalah area yang sering menarik organisasi karena umumnya ada jauh lebih banyak undang-undang dan peraturan yang berdampak pada organisasi daripada yang pertama kali dipertimbangkan. Auditor akan mencari untuk melihat bagaimana organisasi telah mengidentifikasi dan mencatat kewajiban hukum, peraturan dan kontraknya; tanggung jawab untuk memenuhi persyaratan tersebut dan segala kebijakan, prosedur, dan kontrol lain yang diperlukan untuk memenuhi kontrol tersebut. Selain itu, mereka akan melihat bahwa daftar ini dikelola secara teratur terhadap setiap perubahan yang relevan - terutama dalam undang-undang di bidang umum yang mereka harapkan akan dipengaruhi oleh organisasi mana pun.

Hak kekayaan intelektual

Kontrol yang baik menjelaskan bagaimana prosedur yang sesuai memastikan kepatuhan terhadap persyaratan legislatif, peraturan, dan kontrak terkait dengan hak kekayaan intelektual dan penggunaan produk perangkat lunak berpemilik. Sederhananya, organisasi harus menerapkan prosedur yang tepat yang memastikan kepatuhan terhadap semua persyaratannya, apakah itu legislatif, peraturan atau kontrak - terkait dengan penggunaan produk perangkat lunak atau hak kekayaan intelektual.

Ada dua aspek manajemen HKI yang perlu dipertimbangkan; Perlindungan HKI yang dimiliki oleh organisasi; dan Pencegahan penyalahgunaan atau pelanggaran HAKI lainnya. Yang pertama juga akan dibahas dengan A.13.24 untuk perjanjian non-pengungkapan dan kerahasiaan, di mana kami juga menyarankan perusahaan mengelola kontrak induk yang lebih luas dengan pihak ketiga dari, dan juga dalam A.15 untuk rantai pasokan secara khusus. Untuk staf, A7.1.2. Syarat dan ketentuan kerja juga akan mencakup HKI.

Kebijakan, proses, dan kontrol teknis mungkin diperlukan untuk kedua aspek ini. Di dalam register aset dan kebijakan penggunaan yang dapat diterima, kemungkinan bahwa pertimbangan HKI perlu dibuat - mis. di mana aset berada atau mengandung perlindungan HKI aset ini harus mempertimbangkan aspek HKI. Kontrol untuk memastikan bahwa hanya perangkat lunak resmi dan berlisensi yang digunakan dalam organisasi harus mencakup inspeksi dan audit berkala.

Auditor akan ingin melihat bahwa register lisensi yang dimiliki oleh organisasi untuk penggunaan perangkat lunak orang lain dan aset lainnya disimpan dan diperbarui. Yang menarik bagi mereka adalah memastikan bahwa di mana lisensi mencakup jumlah maksimum pengguna atau instalasi, bahwa jumlah ini tidak terlampaui dan nomor pengguna dan instalasi diaudit secara berkala untuk memeriksa kepatuhan. Auditor juga akan melihat bagaimana organisasi melindungi HKI-nya sendiri, yang mungkin termasuk; Kehilangan data dan kontrol pencegahan; Kebijakan dan program kesadaran yang menargetkan pendidikan pengguna; atau Perjanjian non-pengungkapan dan kerahasiaan yang terus berlanjut setelah pemutusan hubungan kerja.

Perlindungan Catatan

Kontrol yang baik menjelaskan bagaimana catatan dilindungi dari kehilangan, kehancuran, pemalsuan, akses yang tidak sah, dan rilis yang tidak sah, sesuai dengan persyaratan perundang-undangan, peraturan, kontrak, dan bisnis. Berbagai jenis catatan kemungkinan akan membutuhkan tingkat dan metode perlindungan yang berbeda. Sangat penting bahwa catatan secara memadai dan proporsionalitas dilindungi terhadap kehilangan, kehancuran, pemalsuan, akses atau pelepasan yang tidak sah. Perlindungan catatan harus mematuhi hukum, peraturan, atau kewajiban kontrak yang relevan. Sangat penting untuk memahami berapa lama catatan harus, harus atau dapat disimpan untuk dan apa masalah teknis atau fisik yang mempengaruhi ini dari waktu ke waktu - mengingat bahwa beberapa undang-undang mungkin mengalahkan yang lain untuk penyimpanan dan perlindungan. Auditor akan memeriksa untuk melihat bahwa pertimbangan untuk perlindungan catatan telah dibuat berdasarkan persyaratan bisnis, hukum, peraturan, dan kewajiban kontraktual.

Privasi & Perlindungan Informasi Identifikasi Pribadi

Kontrol yang baik menjelaskan bagaimana privasi dan perlindungan informasi yang dapat diidentifikasi secara pribadi dijamin untuk perundang-undangan dan peraturan yang relevan. Setiap informasi yang ditangani yang berisi informasi pengenal pribadi (PII) kemungkinan akan tunduk pada kewajiban peraturan perundang-undangan. PII sangat mungkin memiliki persyaratan tinggi untuk kerahasiaan dan integritas, dan dalam beberapa kasus ketersediaan juga (mis. Informasi kesehatan, informasi keuangan). Di bawah beberapa undang-undang (mis. GDPR) beberapa jenis PII didefinisikan sebagai “sensitif” tambahan dan membutuhkan kontrol lebih lanjut untuk memastikan kepatuhan.

Penting bahwa kampanye penyadaran digunakan bersama staf dan pemangku kepentingan untuk memastikan pemahaman berulang tentang tanggung jawab individu untuk melindungi PII dan privasi. Auditor akan mencari untuk melihat bagaimana PII ditangani, jika kontrol yang sesuai telah dilaksanakan, apakah mereka sedang dipantau, ditinjau dan jika perlu ditingkatkan. Mereka juga akan mencari untuk memeriksa bahwa persyaratan penanganan dipenuhi, dan diaudit sesuai. Tanggung jawab tambahan juga ada, misalnya GDPR akan mengharapkan audit rutin untuk bidang-bidang di mana data pribadi berisiko. Organisasi cerdas akan mengikat audit ini di samping audit ISO 27001 mereka dan menghindari duplikasi atau kesenjangan.

Referensi

<https://www.isms.online/iso-27001/annex-a-18-compliance/>

<https://www.isms.online/iso-27001/annex-a-17-information-security-aspects-of-business-continuity-management/>

<https://www.isms.online/iso-27001/annex-a-16-information-security-incident-management/>

<https://www.isms.online/iso-27001/annex-a-14-system-acquisition-development-and-maintenance/>

<https://advisera.com/27001academy/blog/2015/07/27/how-to-handle-access-control-according-to-iso-27001/>

<http://isms-guide.blogspot.com/2007/07/physical-and-environmental-security-iso.html>

<https://www.isms.online/iso-27001/annex-a-7-human-resource-security/>

<https://www.isms.online/iso-27001/annex-a-8-asset-management/>

<https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-in-your-information-security-policy-according-to-iso-27001/>