BAB II

LANDASAN TEORI

2.1 Keamanan Informasi

Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai '*quality or state of being secure-to be free from danger*'. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya. Contoh tinjauan keamanan informasi dari Whitman dan Mattord (2011) sebagai berikut.

a. *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.
b. *Personal Security* yang overlap dengan '*phisycal security'* dalam melindungi orang-orang dalam organisasi
c. *Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
d. *Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
e. *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 diatas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi, termasuk *system* 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 investassi dan peluang usaha.

2.2 Aspek Keamanan Informasi

Perlindungan pada Informasi tersebut dilakukan untuk memenuhi aspek keamanan informasi. Aspek-aspek tersebut seharusnya diperhatikan atau dikontrol dan semestinya dipahami untuk diterapkan Whitman dan Mattord (2009) menyebutkan beberapa aspek yang terkait dengan keamanan informasi yang akan dijelaskan sebagai berikut:

a. *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 informasi dari orang lain.

b. *Identification*

   Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi umumnya dilakukan dengan penggunaan *user name* dan *user ID.*

c. *Authentication*

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

d. *Authorization*

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

e. *Accountability*

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

Keamanan informasi terdiri dari perlindungan terhadap aspek *Confidentiality, Integrity dan Avalability* yang terdapat pada Gambar 2.1.

a. *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.

b. *Integrity* (integritas)

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

c. *Availability* (ketersediaan)

Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan,

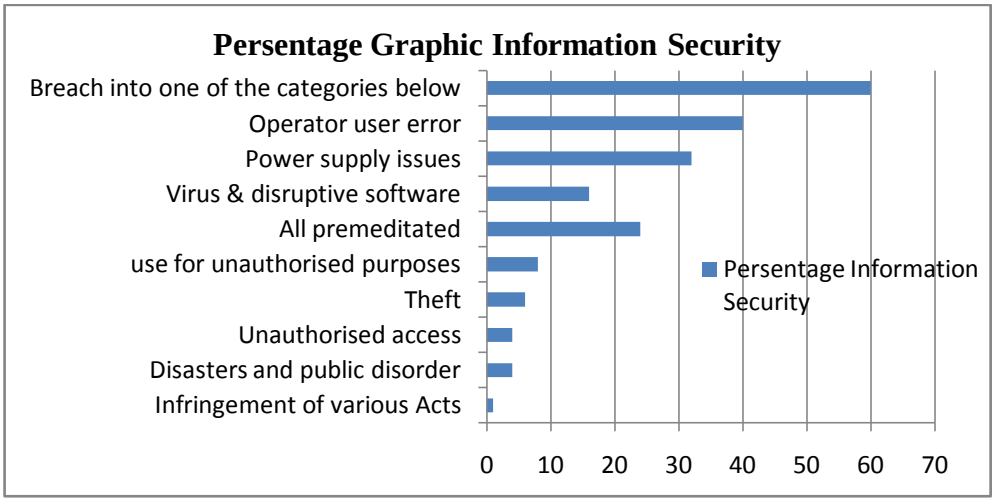
memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

Gambar 2.1 Elemen-elemen Keamanan Informasi
(Sumber: Sarno dan Iffano, 2009)

2.3 Alasan Dibutuhkan Keamanan Informasi

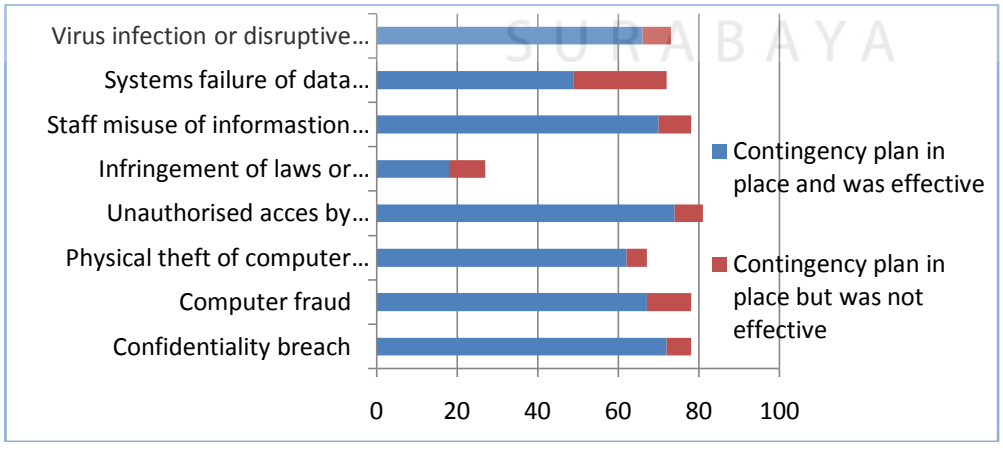
Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil kerugian perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar. Hasil survey ISBS tahun 2000 menunjukkan bahwa sebagian besar data atau informasi tidak cukup terpelihara atau terlindungi sehingga menimbulkan kerawanan. Hasil survei yang terkait dengan hal ini dapat dilihat pada Gambar 2.2.

Survei pada Gambar 2.2 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%).



Gambar 2.2 Grafik Persentase Ancaman Keamanan Informasi ISBS 2000

Survei ISBS (2012) pada Gambar 2.3 menunjukkan bahwa ancaman keamanan informasi yang masih banyak ditemukan adalah mengenai SDM, proses dan teknologi itu sendiri. Setiap tahun jumlah pelanggaran terhadap keamanan informasi akan semakin meningkat karena diikuti juga mengenai perkembangan teknologi yang semakin maju. Untuk itulah maka haruslah ada mengenai suatu pengontrolan keamanan informasi.

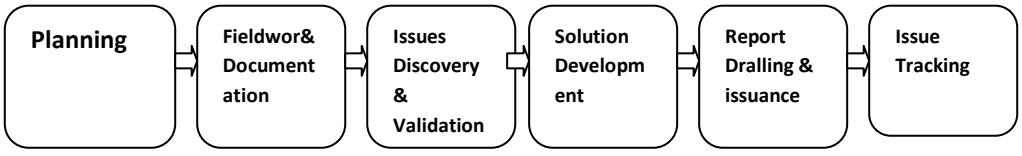


Gambar 2.3 Grafik Persentase Ancaman Keamanan Informasi ISBS 2012

Menurut Lin, dkk (2011) bahwa dengan mengetahui ilmu dan pengetahuan mengenai pengontrolan keamanan informasi yang saat ini sedang diimplementasikan dalam organisasi, seseorang dapat menetapkan pedoman organisasi untuk perusahaan sehingga dapat efektif dalam pengelolaan keamananan informasi. Dalam meningkatkan sistem pengendalian internal dan keamanan informasi pada organisasi dapat membantu organisasi dalam meningkatkan keamanan informasi.

2.4 Audit Keamanan Sistem Informasi

Audit adalah proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti *(audit evidence)* dan dievaluasi secara *obyektif* untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan ISACA dalam Sarno (2009). Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimasi risiko dan memaksimalkan atau mempercepat pengambilan invenstasi dan peluang bisnis (ISO/IEC 27001, 2005).



Gambar 2.4 Gambaran Proses Audit menurut Davis (Davis dkk, 2011:43)

Menurut Davis, dkk (2011) tahapan audit seperti yang terlihat pada Gambar 2.4 yang setiap tahapan-tahapan akan dijelaskan sebagai berikut.

1. *Planning*

   Sebelum melakukan audit terlebih dahulu harus menentukan rencana meninjau bagaimana audit dilakukan. Jika proses perencaaan dilakukan secara efektif, maka dapat membentuk tim audit yang dapat berjalan dengan baik. Sebaliknya, jika itu dilakukan dengan buruk serta pekerjaan dimulai tanpa rencana yang jelas tanpa arah, upaya tim audit dapa mengakibatkan kegagalan tujuan dari proses perencaaan adalah menentukan tujuan dan ruang lingkup audit, yaitu harus menentukan apa yang akan dicapai.

2. *Fieldwork and Documentation*

   Sebagian besar audit terjadi selama fase ini, ada saat pemeriksaan langkah-langkah yang dibuat selama tahap sebelumnya dijalankan oleh tim audit. Saat ini tim audit teleh memperoleh data dan melakukan wawancara yang akan membantu anggota tim untuk menganalisis potensi risiko dan menentukan risiko belum dikurangi dengan tepat. Auditor juga harus melakukan pekerjaan yang dapat mendokumentasikan pekerjaan mereka sehingga kesimpulan dapat dibuktikan. Tujuan mendokumentasikan pekerjaan harus cukup detail sehingga cukup informasi bagi orang untuk dapat memahami apa yang dilakukan dan tersampainya kesimpulan yang sama seperti auditor.

3. *Issues Discovery and Validation*

   Pada tahap ini auditor harus menentukan dan melakukan perbaikan pada daftar isu-isu yang potensial untuk memastikan isu-isu yang valid pada relevan. Auditor harus mendiskusikan isu-isu potensial dengan pelanggan secepat mungkin. Selain memvalidasi bahwa fakta-fakta telah benar, maka

perlu memvalidasi bahwa risiko yang disajikan oleh masalah ini cukup signifikan memiliki nilai untuk pelaporan dan pengalamatan.

4. *Solution Development*

Setelah mengidentifikasikan isu-isu potensial di wilayah yang sedang dilakukan audit dan telah memvalidasi fakta dan risiko, maka dapat dilakukan rencanan untuk mengatasi setiap masalah. Tentu, hanya mengangkat isu-isu yang tidak baik bagi perusahaan dan isu isu yang benar benar harus ditangani. Tiga pendekatan umum yang digunakan untuk mengembangkan tindakan dalam menangani masalah audit adalah sebagai berikut.

a. Pendekatan rekomendasi
b. Pendekatan respon manajemen
c. Pendekatan solusi

5. *Report Drafting and Issuance*

Setelah ditemukan masalah dalam lingkungan yang diaudit, memvalidasi, dan mendapatkan solusi yang dikembangkan untuk mengatasi masalah, maka dapat membuat draf untuk laporan audit. Laporan audit adalah sebagai dokumen hasil audit. Fungsi utama laporan audit adalah sebagai berikut.

a. Untuk auditor dan perusahaan yang diaudit, berfungsi sebagai catatan audit, hasilnya, dan rencana rekomendasi yang dihasilkan.
b. Untuk manajemen senior dan komite audit, berfungsi sebagai "kartu laporan" pada daerah yang telah diaudit.

6. *Issue Tracking*

Audit belum benar-benar lengkap sampai isu yang diangkat dalam audit tersebut diselesaikan. Departemen harus mengembangkan suatu proses

dimana anggotanya dapat melacak dan mengikuti sampai isu terselesaikan. Auditor yang melakukan atau memimpin audit bertanggung jawab untuk menindak lanjuti poin dari audit seperti tanggal jatuh tempo untuk setiap pendekatan dari audit yang dihasilkan.

Contoh dari Keamanan Informasi yakni:

a. *Physical Security* adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
b. *Personal Security* adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup *'physical security'*.
c. *Operation Security* adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
d. *Communications Security* adalah keamanan informasi bertujuan mengamankan media komunikasi, teknologi komunikasi, serta apa yang ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
e. *Network Security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringan, data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Audit Sistem Informasi adalah prosess mengumpulkan dan mengevaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien (Weber, 1999).

Beberapa elemen utama tinjauan penting dalam Audit Sistem Informasi yaitu dapat diklasifikasikan sebagai berikut:

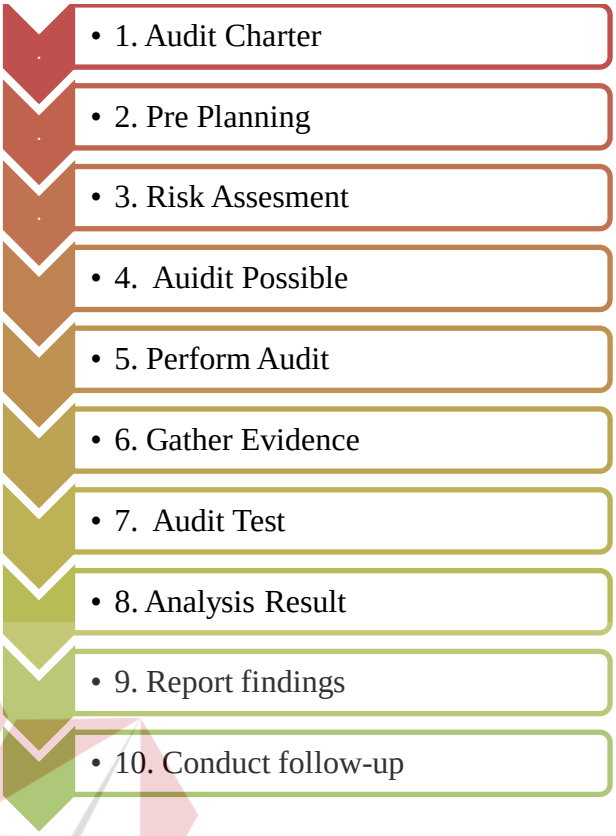
1. Tinjauan terkait dengan fisik dan lingkungan, yaitu: hal-hal yang terkait dengan keamanan fisik, suplai sumber daya, temperatur, kontrol kelembaban dan faktor lingkungan lain.
2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen database, seluruh prosedur administrasi sistem dan pelaksanaannya.
3. Tinjauan perangkat lunak. Perangkat lunak yang dimaksud merupakan aplikasi bisnis. Mencakup kontrol akses dan otorisasi ke dalam sistem, validasi dan penanganan kesalahan termasuk pengecualian dalam sistem serta aliran proses bisnis dalam perangkat lunak beserta kontrol secara manual dan prosedur penggunaannya. Sebagai tambahan, tinjauan juga perlu dilakukan terhadap siklus hidup pengembangan sistem.
4. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan sistem, batasan tingkat keamanan, tinjauan terhadap *firewall*, daftar kontrol akses router, *port scanning* serta pendeteksian akan gangguan maupun ancaman terhadap sistem.

5. Tinjauan kontinuitas bisnis dengan memastikan ketersediaan prosedur *backup* dan penyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana/kontinuitas bisnis yang dimiliki.
6. Tinjauan integritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

2.5 Langkah-Langkah Audit TI

Sebelum mengetahui langkah-langkah dari audit maka harus mengenal terlebih dahulu mengenai auditor dan auditti. Auditor adalah orang yang melakukan audit untuk mendapatkan bukti yang akurat sesuai dengan yang telah ditetapkan dan melaporkan hasilnya kepada para pihak yang berkepentingan. Auditee adalah seseorang yang diaudit atau diperiksa oleh auditor untuk mendapatkan informasi yang dibutuhkan dalam upaya untuk mencapai tujuan yang diinginkan (Haryono, 2001).

Banyak berbagai macam versi dan jenis dalam menjalankan tahapan audit. Terdapat 10 tahapan yang dilakukan dalam proses audit, yaitu: 1. Membuat dan Mendapatkan Surat Persetujuan Audit, 2. Perencanaan Audit, 3.Analisis Risiko, 4. Persiapan Audit, 5. Pelaksanaan Audit, 6. Pemeriksaaan Data dan Bukti, 7. Tes Audit, 8. Pemeriksaaan Hasil Audit, 9. Pelaporan Audit, 10. Pertemuan Penutup. Tahapan tersebut dapat dilihat pada Gambar 2.4.



Gambar 2.5 Langkah-Langkah Audit Teknologi Informasi
(Sumber: CISA, 2011)

2.6 Standar Sistem Manajemen Keamanan Informasi

Sejak tahun 2005, *International Organization for Standardization* (ISO) atau organisasi Internasional untuk standarisasi telah mengembangkan sejumlah standar tentang *Information Security Management System* (ISMS). Standar SMKI ini dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri dari:

a. ISO/IEC 27000: 2009 – *ISMS Overview and Vocabulary*

b. ISO/IEC 27001: 2005 – *ISMS Requirement*

c. ISO/IEC 27002: 2005 – *Code of Practice for ISMS*

d. ISO/IEC 27003: 2010 – *ISMS Implementation Guidance*

e. ISO/IEC 27004: 2009 – *ISMS Measuements*

f. ISO/IEC 27005: 2008 – *Information Security Risk Management*

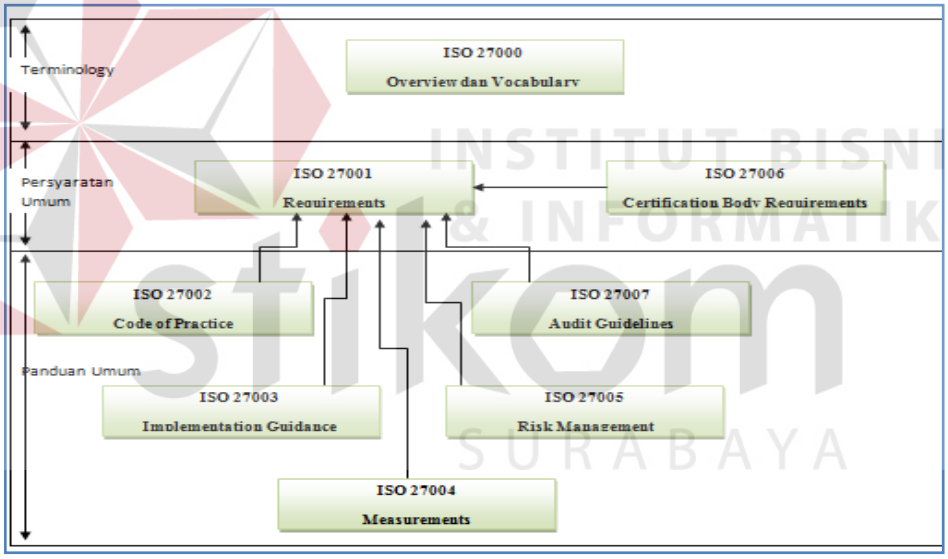
g. ISO/IEC 27006: 2007 – *ISMS Certification Body Requiements*

h. ISO/IEC 27007 – *Guidelines for ISMS Auditing*

Adapun penjelasan dari standar ISMS tersebut dijelaskan sebagai berikut.

a. ISO/IEC 27000:2009 – *ISMS Overview and Vocabulary*

Standar ini dirilis tahun 2009, memuat prinsip-prinsip dasar *Information Security Management System*, definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga SMKI, baik yang telah diterbitkan maupun sedang tahap pengembangan. Hubungan antar standar keluarga ISO 27000 dapat dilihat pada Gambar 2.6.



Gambar 2.6 Hubungan Antar Standar Keluarga SMKI
(Sumber: Direktorat Keamanan Informasi, 2011)

Dari standar seri ISO 27000 hingga September 2011 baru ISO/IEC 27001: 2005 yang telah diadopsi Badan Standardisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) berbahasa Indonesia bernomor SNI ISO/IEC 27001:2009.

b. ISO/IEC 27001:2005 – *ISMS Requirement*

ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi masyarakat penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan.

Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang *(review)*, pemeliharaan dan peningkatan suatu SMKI. Model PLAN – DO – CHECK–ACT (PDCA) diterapkan terhadap struktur keseluruhan proses SMKI. Dalam model PDCA (ISO/IEC 27002, 2005) *– Code of Practice for ISMS)*

c. ISO/IEC 27002: 2005 – *Code of Practice for ISMS*

ISO IEC 17799 tahun 2005, resmi dipublikasikan pada tanggal 15 Juni 2005. Pada tanggal 1 Juli 2007, nama itu secara resmi diubah menjadi ISO IEC 27002 tahun 2005. Konten tersebut masih persis sama. Standar ISO IEC 17799:2005 (sekarang dikenal sebagai ISO IEC 27002:2005) dikembangkan oleh IT *Security Subcommittee* (SC 27) dan *Technical Committee on Information Technology* (ISO/IEC JTC 1) (ISO 27002, 2005).

c. ISO/IEC 27003:2010 – *ISMS Implementation Guidance*

Tujuan dari ISO/IEC 27003 adalah untuk memberikan panduan bagi perancangan dan penerapan SMKI agar memenuhi persyaratan ISO 27001. Standar ini menjelaskan proses pembangunan SMKI meliputi pengarsipan, perancangan dan penyusunan atau pengembangan SMKI yang digambarkan sebagai suatu kegiatan proyek.

d. ISO/IEC 27004:2009 – *ISMS Measuements*

Standar ini menyediakan penyusunan dan penggunaan teknik pengukuran untuk mengkaji efektivitas penerapan SMKI dan kontrol sebagaimana disyaratkan ISO/IEC 27001. Standar ini juga membantu organisasi dalam mengukur ketercapaian sasaran keamanan yang ditetapkan.

e. ISO/IEC 27005:2008 – *Information Security Risk Management*

Standar ini menyediakan panduan bagi kegiatan manajemen risiko keamanan informasi dalam suatu organisasi, khususnya dalam rangka mendukung persyaratan- persyaratan SMKI sebagaimana didefinisikan oleh ISO/IEC 27001. Standar ini diterbitkan pada bulan Juni 2008.

f. ISO/IEC 27006:2007–*ISMS Certification Body Requiements*

Standar ini menetapkan persyaratan dan memberikan panduan bagi organisasi yang memiliki kewenangan untuk melakukan audit dan sertifikasi SMKI. Standar ini utamanya dimaksudkan untuk mendukung porses akreditasi Badan Sertifikasi ISO/IEC 27001 oleh Komite Akreditasi dari negara masing-masing.

g. ISO/IEC 27007–*Guidelines for ISMS Auditing*

Standar ini memaparkan penduan bagaimana melakukan audit SMKI perusahaan.

2.7 ISO/IEC 27002: 2005

ISO 27002: 2005 adalah standar keamanan informasi sebagai *best practice* atau panduan umum yang menjelaskan adanya contoh penerapan keamanan informasi dengan menggunakan bentuk kontrol sehingga dapat mencapai sasaran yang diterapkan. Standar ini dapat digunakan sebagai titik awal dalam penyusunan dan pengembangan ISMS. Standar ini memberikan panduan dalam perencanaan dan implementasi suatu program untuk melindungi aset-aset informasi.

Hubungan ISO/IEC 27001 dengan ISO/IEC 27002: 2005 secara resmi mendefinisikan persyaratan wajib untuk Sistem Manajemen Keamanan Informasi (SMKI). ISO / IEC 27002: 2005 menunjukkan kontrol keamanan informasi yang sesuai dalam ISMS yang digunakan sebagai kode praktek atau pedoman pelaksanaan kontrol keamanan informasi. ISO / IEC 27001 mencakup ringkasan dari kontrol dari ISO / IEC 27002: 2005.

ISO 27002: 2005 menyediakan rekomendasi *best practice* terhadap manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab untuk proses inisiasi, implementasi, dan pemeliharaan *Information Security Management Systems* (ISMS) pada suatu organisasi. ISO 27002: 2005 menerapkan kontrol keamanan dimana pengontrolannya tersaji dalam bentuk 12 kontrol area, 41 kontrol objektif, dan 133 kontrol yang dapat dilihat pada Tabel 2.1.

Tabel 2.1 Ringkasan Jumlah Klausul Kontrol Keamanan, Objektif Kontrol dan Kontrol pada ISO 27002:2005.

Klausul	Jumlah	
	Objektif Kontrol	Kontrol
4	2	-
5	1	2
6	2	11
7	2	5
8	3	9
9	2	13
10	10	32
11	7	25
12	6	16
13	2	5
14	1	5
15	3	10
Jumlah: 12	Jumlah: 41	Jumlah:133

Sedangkan untuk detail struktur kontrol keamanan dari ISO/IEC 27002:2005 dapat dilihat pada Tabel 2.2.

Tabel 2.2. Detail Struktur Kontrol Keamanan ISO/IEC 27002: 2005

Klausul : 4 Dugaan Risiko dan Perawatannya
Kategori Keamanan Utama: 4.1 Perkiraan Risiko Keamanan
Kategori Keamanan Utama : 4.2 Perawatan Risiko Keamanan
Klausul : 5 Kebijakan Keamanan
Kategori Keamanan Utama: 5.1 Kebijakan Keamanan Informasi Objektif Kontrol: Memberikan arahan kepada manajemen organisasi dan dukungan untuk Keamanan Informasi dalam hubungannya dengan persyaratan bisnis organisasi dan aturan yang sedang berlaku.
Kontrol: 5.1.1 Dokumen Kebijakan Keamanan Informasi
Kontrol : 5.1.2 Tinjauan Ulang Kebijakan Keamanan Informasi
Klausul: 6 Organisasi Keamanan Informasi
Kategori Keamanan Utama: 6.1 Organisasi Internal
Objektif Kontrol: Bagaimana mengelola Keamanan Informasi di dalam organisasi
Kontrol: 6.1.1 Komitmen Pihak Manajemen Terhadap Keamanan Informasi
Kontrol: 6.1.2 Koordinasi Keamanan Informasi
Kontrol: 6.1.3 Pembagian Tanggung Jawab Keamanan Informasi
Kontrol: 6.1.4 Proses Otorisasi Untuk Akses Ke Fasilitas Pemrosesan Informasi
Kontrol: 6.1.5 Perjanjian Kerahasiaan
Kontrol: 6.1.6 Hubungan Dengan Pihak-Pihak (Vendor) Legal
Kontrol: 6.1.7 Hubungan Dengan Lembaga-Lembaga atau Organisasi Tertentu
Kontrol: 6.1.8 Kaji Ulang Secara Independen Keamanan Informasi

Tabel 2.2. Detail Struktur Kontrol Keamanan ISO/IEC 27002: 2005 (Lanjutan)

Klausul: 6 Organisasi Keamanan Informasi
Kategori Keamanan Utama: 6.2 Pihak Internal
Objektif Kontrol: Untuk menjaga Keamanan Informasi dan fasilitas pemrosesan informasi organisasi yang diakses, diproses, dikomunikasikan atau dikelola oleh pihak ketiga
Kontrol: 6.2.1 Identifikasi Risiko Terhadap Hubungannya Dengan Pihak Ketiga
Kontrol: 6.2.2 Akses Keamanan Dalam Hubungan Dengan Pelanggan
Kontrol: 6.2.3 Melibatkan Persyaratan Keamanan Dalam Perjanjian Dengan Pihak Ketiga
Klausul: 7 Manajemen Aset
Kategori Keamanan Utama: 7.1 Tanggung Jawab Aset
Objektif Kontrol: Untuk memenuhi perlindungan dan pemeliharaan terhadap aset organisasi
Kontrol: 7.1.1 Inventarisasi Aset
Kontrol: 7.1.2 Kepemilikan Aset
Kontrol: 7.1.3 Penggunaan Aset yang Diterima
Kategori Keamanan Utama: Klasifkasi Informasi
Objektif Kontrol: Untuk memastikan bahwa setiap Informasi dalam organisasi mendapatkan keamanan yang memadai.
Kontrol: 7.2.1 Pedoman Klasifikasi
Kontrol: 7.2.2 Informasi Pelabelan dan Penanganan
Klausul: 8 Keamanan Sumber Daya Manusia
Kategori Keamanan Utama: 8.1 Sebelum Menjadi Pegawai
Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga memahami akan tanggung jawabnya dan bisa menjalankan aturan yang mereka dapatkan untuk meminimalkan risiko pencurian atau kesalahan dalam penggunaan fasilitas informasi.
Kontrol: 8.1.1 Peran dan tanggung Jawab
Kontrol: 8.1.2 Penyaringan
Kontrol: 8.1.3 Syarat dan Kondisi Kerja
Kategor i Keamanan Utama: 8.2 Selama Menjadi pegawai
Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga memahami Keamanan Informasi yang telah ditetapkan oleh organisasi demi mengurangi terjadinya kesalahan kerja *(human error)* dan risiko yang dihadapi oleh organisasi.
Kontrol: 8.2.1 Tanggung Jawab Manajemen
Kontrol: 8.2.2 Kesadaran Keamaan Informasi, Pendidikan dan Pelatihan
Kontrol: 8.2.3 Pemberhentian Tanggung Jawab

Tabel 2.2 Detail Struktur Kontrol Keamanan ISO/IEC 27002: 2005 (Lanjutan)

Kategori Keamanan Utama: 8.3 Pemberhentian dan Pemindahan Pegawai. Objektif Kontrol: Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga yang diberhentikan dipindah dilakukan sesuai dengan prosedur yang benar.
Kontrol: 8.3.1 Pemberhentian Taggung Jawab
Kontrol: 8.3.2 Pengembalian Aset
Kontrol: 8.3.3 Penghapusan Hak Akses
Klausul: 9 Keamanan Fisik dan Lingkungan
Kategori Keamanan Utama: 9.1 Daerah Aman
Objektif Kontrol: Untuk mencegah akses fisik tanpa hak, kerusakan dan gangguan terhadap Informasi dan perangkatnya dalam organisasi.
Kontrol: 9.1.1 Keamanan Perimeter
Kontrol: 9.1.2 Kontrol Entri Fisik
Kontrol: 9.1.3 Keamanan Kantor, Ruang dan Fasilitasnya
Kontrol: 9.1.4 Perlidungan Terhadap Ancaman Dari Luar dan Lingkungan Sekitar
Kontrol; 9.1.5 Bekerja di Wilayah Aman
Kontrol: 9.1.6 Akses Publik, Tempat Pengiriman dan Penurunan Barang
Kategori Keamanan Utama: 9.2. Peralatan Keamanan. Objektif Kontrol: Untuk mencegah kehilangan, kerusakan, pencurian atau ketidaberesan aset dan gangguan tehadap aktivitas organisasi.
Kontrol: 9.2.1 Penempatan dan Perlindungan Peralatan
Kontrol: 9.2.2 Peralatan Pendukung
Kontrol: 9.2.3 Keamanan Kabel
Kontrol: 9.2.4 Pemeliharaan Peralatan
Kontrol: 9.2.5 Keamanan Peralatan Diluar Area
Kontrol: 9.2.6 Penggunaan Ulang Peralatan
Kontrol: 9.2.7 Pemindahan Peralatan
Klausul: 10 Manajemen Komunikasi dan Operasi
Kategori Keamanan Utama: 10.1 Tanggung Jawab dan Prosedur Operasional Objektif Kontrol: Untuk memastikan keamanan operasi dan tidak terjadi kesalahan dalam mengoperasikan fasilitas-faslitas pemrosesan Informasi
Kontrol: 10.l.1 Pendokumentasian Prosedur Operasi
Kontrol 10.1.2 Manajemen Pertukaran
Kontrol 10.1.3 Pemisahan Tugas
Kontrol: 10.1.4 Pemisahan Pengembangan, Pengujian dan Operasional Informasi
Kategori Keamanan Utama: 10.2 Manajemen Pengiriman Oleh Pihak Ketiga
Objektif Kontrol: Untuk mengimplementasikan dan memelihara Keamanan Informasi yang sesuai dalam hal layanan pengiriman yang berhubungan dengan perjanjain layanan pengiriman dengan pihak ketiga.
Kontrol: 10.2.1 Layanan Pengiriman
Kontrol: 10.2.2 Pemantauan dan Pengkajian Ulang Layanan Pihak Ketiga
Kontrol: 10.2.3 Manajemen Penggantian Layanan Pihak Ketiga

Tabel 2.2 Detail Struktur Kontrol Keamanan ISO/IEC 27002: 2005 (Lanjutan)

Kategori Keamanan Utama: 10.3 Perencanaan Sistem dan Penerimaan Objektif Kontrol: Untuk meminimalisasi kegagalan sistem.
Kontrol: 10.3.1 Manajemen Kapasitas
Kontrol: 10.3.2 Penerimaan Sistem
Kategori Keamanan Utama: 10.4 Perlindungan Terhadap *Malicious dan Mobile Code*
Objektif Kontrol: Untuk melindungi integritas perangkat lunak (software) dan Informasi.
Kontrol: 10.4.1 Kontrol Terhadap Kode Berbahaya (*Maliciious Code)*
Kontrol: 10.4.2 Koontrol Terhadap *Mobile Code*
Katagori Keamanan Utama: 10.5 *Backup* Objektif Kontrol: Untuk memelihara integritas dan ketersediaan Informasi dan faslitas pemrosesan Informasi.
Kontrol: 10.5.1 Back-up Informasi
Katagori Keamanan Utama: 10.6 Manajemen Keamanan Jaringan Objektif Kontrol: Untuk memelihara keamanan pengiriman Informasi di jaringan serta melindungi infrastruktur pendukungnya
Kontrol: 10.6.1 Kontrol Jaringan
Kontrol: 10.6.2 Keamanan Dalam Layanan Jaringan
Kategori keamanan Utama: 10.7 Penanganan Media Objektif Kontrol: Untuk mencegah pengaksesan, modifikasi, penghapusan atau pengrusakan aset secara ilegal serta gangguan aktifitas bisnis
Kontrol: 10.7.1 Manajemen Pemindahan Media
Kontrol: 10.7.2 Pemusnahan atau Pembuangan Media
Kontrol: 10.7.3 Prosedur Penanganan Informasi
Kontrol: 10.7.4 Keamanan Dokumentasi Sistem
Katagori Keamanan Utama: 10.8 Pertukaran Informasi Objektif Kontrol: Untuk memelihara keamanan pertukaran informasi dan perangkat lunak didalam organisasi dengan pihak luar.
Kontrol: 10.8.1 Kebijakan dan Prosedur Pertukaran informasi
Kontrol: 10.8.2 Perjanjian Pertukaran
Kontrol: 10.8.3 Transportasi Media Fisik
Kontrol: 10.8.4 Pesan Elektronik
Kontrol: 10.8.5 Sistem Informasi Bisnis
Kategori keamanan Utamal 10.9 Layanan E-Commerce Objektif Kontrol: Untuk memastikan keamanan dalam layanan dan penggunaan E-Commerce
Kontrol: 10.9.1 E-commerce
Kontrol: 10.9.2 Transaksi On-Line
Kontrol: 10.9.3 Informasi Untuk Publik

Tabel 2.2 Detail Struktur Kontrol Keamanan ISO/IEC 27002: 2005 (Lanjutan)

Kategori Keamanan Utama: 10.10 Monitoring Objektif Kontrol: Untu mendeteksi aktifitas pemrosesan informasi.
Kontrol: 10.10.1 Rekaman Audit
Kontrol: 10.10.2 Monitoritng Penggunaan Sistem
Kontrol: 10.10.3 Proteksi Catatan informasi
Kontrol: 10.10.4 Catatan Administratir dan Operator
Kontrol: 10.10.5 Catatan Kesalahan
Kontrol: 10.10.6 Sinkronisasi Waktu
Klausul: 11 Kontrol Akses
Kategori Keamanan Utama: 11.1 Kebijakan Kontrol Akses Objektif Kontrol: Untuk megontrol akses informasi.
Kontrol: 11.1.1 Kebijakan Kontrol Akses
Kategori Keamanan Utama: 11.2 Manajemen Akses Uset Objektif Kontrol: Untuk memastikan pengguna yang mempunyai hak akses ke Sistem Informasi dan yang tidak.
Kontrol: 11.2.1 Registrasi Pengguna
Kontrol: 11.2.2 Manajemen Hak Istimewa
Kontrol: 11.2.3 Manajemen *Password* User
Kategori Keamanan Utama: 11.2 Manajemen Akses user Objektif Kontrol: Untuk memastikan pengguna yang mempunyai hak akses ke Sistem Informasi dan yang tidak
Kontrol: 11.2.4 Ulasan Hak Akses Pengguna
Kategori Keamanan Utama: 11.3 Tanggung Jawab Pengguna Objektif Kontrol: Untuk mencegah akses user tanpa hak atau pencurian Informasi dan fasilitas pemrosesan Informasi
Kontrol: 11.3.1 Penggunaan *Password*
Kontrol: 11.3.2 Peralatan Pengguna Yang Tidak Dijaga
Kontrol: 11.3.3 Kebijakan Kerapian Meja dan Penyaringan
Kategori Keamanan Utama: 11.4 Kebijakan Penggunaan Layanan Jaringan Objektif Kontrol: Untuk mencegah akses tanpa hak kedalam layanan jaringan.
Kontrol: 11.4.1 Kebijakan Penggunaan Layanan jaringan
Kontrol : 11.4.2 Otentikasi Pengguna Koneksi eksternal.
Kontrol: 11.4.3 Indikasi Peralatan Didalam Jaringan
Kontrol: 11.4.4 Diagnostik Jarak Jauh dan Perlindungan Port Konfigurasi
Kontrol: 11.4.5 Pemisahan jaringan
Kontrol: 11.4.6 Kontrol terhadap koneksi Jaringan
Kontrol: 11.4.7 Kontrol Terhadap Routing Jaringan

Tabel 2.2 Detail Struktur Kontrol Keamanan ISO/IEC 27002: 2005 (Lanjutan)

Kategori Keamanan Utama: 11.5 Kontrol Akses Sistem Operasi Objektif Kontrol: Untuk mencegah akses tanpa hak ke sistem operasi
Kontrol: 11.5.1 Prosedur log-on yang aman
Kontrol: 11.5.2 Identifkasi dan Otentikasi User
Kontrol: 11.5.3 Manajemen Password
Kontrol: 11.5.4 Sistem Peralatan Pengguna
Kontrol: 11.5.5 Sesi Time-Out
Kontrol: 11.5.6 Batasan Waktu Koneksi
Kategori Keamanan Utama: 11.6 Kontrol Akses Aplikasi Objektif Kontrol: Untuk mencegah akses tanpa hak terhadap Informasi didalam aplikasi.
Kontrol: 11.6.1 Pembatasan Akses Informasi
Kontrol: 11.6.2 Isolasi Sistem Yang Sensitif
Kategori Keamanan Utama: 11.7 Komputasi Bergerak dan Komunikasi Mobile Objektif Kontrol: Untuk memastikan Keamanan Informasi saat menggunakan fasilitas komputer bergerak atau bekerja dari lain tempat
Kontrol: 11.7.1 Komunikasi dan Terkomputerisasai yang bergerak
Kontrol: 11.7.2 Teleworking
Klausul: 12 Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan
Kategori Keamanan Utama: 12.1.1 Analisis dan Spesifikasi Persyaratan Keamanan.
Objektif Kontrol: Untuk memastikan bahwa keamanan adalah bagian dari Sistem Informasi
Kontrol: 12.1.1Analisa dan Spesifikasi Persyaratan Keamanan
Kategori Keamanan Utama: 12.2 Pemrosesan Yang Benar Dalam Aplikasi Objektif Kontrol: Untuk mencegah kesalahan, kehilangan, modifikasi tanpa hak atau kesalahan penanganan informasi dalam aplikasi.
Kontrol: 12.2.1 Validasi Data Input
Kontrol: 12.2.2 Kontrol Untuk Pemrosesan Internal
Kontrol: 12.2.3 Integritas Pesan
Kontrol: 12.2.4 Validasi Data Output
Kategori Keamanan Utama: 11.2.3 Kontrol Kriptografi Objektif Kontrol: Untuk melindungi Kerahasiaan, Autentikasi dan Keutuhan Informasi dengan menggunakan sistem kriptografi
Kontrol: 12.3.1 Kebijakan Dalam Penggunaan Kriptografi
Kontrol: 12.3.2 Manajemen Kunci
Kategori Keamanan Utama: 12.4 Keamanan File Sistem Objektif Kontrol: Untuk memastikan keamanan file sistem
Kontrol: 12.4.1 Kontrol Operasional Software
Kontrol : 12.4.2 Perlindungan Data Pengujian Sistem
Kontrol: 12.4.3 Kontrol Akses ke Sumber Program

Tabel 2.2 Detail Struktur Kontrol Keamanan ISO/IEC 27002: 2005 (Lanjutan)

Kategori Keamanan Utama: 12.5 Keamanan dalam Pengembangan Proses Pendukunng Objektif Kontrol: Untuk memelihara keamanan Informasi dan Aplikasi Sistem Software
Kontrol: 12.5.1 Prosedur Perubahan Kontrol
Kontrol: 12.5.2 Tinjauan Teknis Aplikasi Setelah Dilakukan Perubahan Sistem Operasi
Kontrol: 12.5.3 Pembatasan Perubahan Paket Software
Kontrol: 12.5.4 Kelemahan Informasi
Kontrol: 12.5.5 Pengembangan perangkat Lunak *Outsourcing*
Kategori Keamanan Utama: 12.6 Manajemen Teknis Kelemahan Objektif Kontrol: Untuk mengurangi resiko yang disebabkan oleh terpublikasinya teknik-teknik kelemahan yang dimiliki.
Kontrol: 12.6.1 Kontrol Terhadap Kelemahan Secara Teknis
Klausul: 13 Manajemen Kejadian Keamanan Informasi
Kategori Keamanan Utama: 13.1 Pelaporan Kejadian dan Kelemahan Keamanan Informasi Objektif Kontrol: Untuk memastikan kejadian dan kelemahan keamanan Sistem Informasi dikomunikasikan dan ditangani tepat waktu.
Kontrol: 13.1.1 Pelaporan Keajadian Keamanan Informasi
Kontrol: 13.1.2 Pelaporan Kelemahan Keamanan
Klausul: 13 Manajemen Kejadian Keamanan Informasi
Kategori Keamanan Utama: 13.2 Manajemen Kejadian Keamanan Informasi dan Pengembangannya Objektif Kontrol: Untuk memastikan konsistensi dan keefektifitasan pendekatan yang diaplikasikan kedalam manajemen kejadian Keamanan Informasi.
Kontrol: 13.2.1 Tanggung jawab dan Prosedur
Kontrol: 13.2.2 Belajar Dari Kejadian Keamanan informasi
Kontrol: 13.2.3 Pengumpulan Bukti
Klausul: 14 Manajemen Kelangsungan Bisnis
Kategori Keamanan Utama: 14.1 Aspek Keamanan Dalam Manajemen Kelangsungan Bisnis. Objektif Kontrol: Untuk menghindari gangguan terhadap aktifitas bisnis serta untuk menjaga proses-proses bisnis yang kritis dari kegagalan dan dampak yang lebih besar atau bencana terhadap Sistem Informasi.
Kontrol: 14.1.1 Memasukkan Keamanan Informasi Dalam proses Manajemen Kelangsungan Bisnis
Kontrol: 14.1.2 Kelangsungan Bisnis dan Penilaian resiko
Kontrol: 14.1.3 Pembangunan dan Rencana Kelangsungan yang di dalamnya Meliputi Keamanan informasi
Kontrol: 14.1.4 Kerangka Kerja Rencana Kelangsungan Bisnis
Kontrol: 14.1.5 Pengujian, Pemeliharaan dan Penilaian Ulang Rencana Bisnis

Tabel 2.2 Detail Struktur Kontrol Keamanan ISO/IEC 27002: 2005 (Lanjutan)

Klausul: 15 Kepatuhan
Kategori Keamanan Utama: 15.1 Kepatuhan Terhadap Persyaratan Legal Objektif Kontrol: Untuk mencegah pelanggaran terhadap hukum, perundangan, peraturan atau kewajiban kontrak dan suatu persyaratan keamanan.
Kontrol: 15.1.1 Identifkasi Perundangan yang Dapat Diaplikasikan
Kontrol: 15.1.2 Hak Kekayaan Inteektual
Kontrol: 15.1.3 Perlindungan Dokument Organisasi
Kontrol: 15.1.4 Perlindungan Data dan Kerahaisaan Informasi
Kontrol: 15.1.5 Pencegahan Penyalahgunaan Faslitas Pemrosesan Informasi
Kontrol: 15.1.6 Peraturan Kontrol Kriptografi
Kategori Keamanan Utama: 15.2 Kepatuhan Dengan Kebijakan Keamanan, Standar dan Kepatuhan Teknik. Objektif Kontrol: Untuk memastikan kepatuhan terhadap sistem didalam kebijakan keamanan organisasi dan standar.
Kontrol: 15.2.1 Kepatuhan Dengan Kebijakan Keamanan dan Standar
Kontrol: 15.2.2 Pemeriksaan Kepatuhan Teknik
Kategori Keamanan Utama: 15.2 Audit Sistem Informasi dan Pertimbangan Objektif Kontrol: Untuk memaksimalkan keefektifitasan dan meminimasi interfensi dari atau kedalam proses audit Sistem Informasi
Kontrol: 15.3.1 Kontrol Audit Sistem Informasi
Kontrol: 15.3.2 Perlindungan terhadap Perangkat Audit Sistem Informasi
Kontrol: 14.1.5 Pengujian, Pemeliharaan dan Penilaian Ulang Rencana Bisnis

2.8 Maturity Level

Maturity level atau tingkat kedewasaan menjelaskan hasil analisa gap atau kesenjangan keamanan informasi yang dinilai sesuai dengan kejadian saat ini dalam peringkat kematangan proses pengelolaan pengamanan informasi. Peringkat dalam penilaian tersebut dilakukan dengan menggunakan 6 tingkatan proses berdasarkan metode penilaian indeks keamanan informasi. Indeks keamanan informasi adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang

didefinisikan oleh standar SNI ISO 27001:2009. Hasil evaluasi indeks Keamanan Informasi menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009. (Direktorat Keamanan Informasi, 2011).

Menurut Kemenkominfo (2011) tingkat kematangan proses pengelolaan keamanan informasi dapat diketahui dengan menggunakan *maturity level*. *Maturity* level digunakan karena merupakan model yang mewujudkan pemikiran dasar manajemen proses sehingga tepat untuk mengukur ISO/IEC 27001 sebagai salah satu standar yang dibuat berdasarkan manajemen proses.

SNI ISO/IEC 27001: 2009 adalah standar SMKI atau *Information Security Management System* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha mengimplementasikan konsep keamanan informasi organisasi.

Berikut adalah indeks alat ukur tingkatan proses keamanan informasi untuk menilai kesiapan keamanan informasi di instansi pemerintahan berdasarkan SNI ISO/IEC 27001: 2009 sebagai berikut:

1. Tingkat 0 - Tidak Diketahui (Pasif)
    a. Status kesiapan keamanan informasi tidak diketahui.
    b. Pihak yang terlibat tidak mengikuti atau tidak melaporkan pemeringkatan Indeks KAMI.
2. Tingkat 1 - Kondisi Awal (Reaktif)
    a. Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi.

b. Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan.
c. Kelemahan teknis dan non teknis tidak terdefinisi dengan baik.
d. Pihak yang terlibat menyadari tanggung jawab mereka.

3. Tingkat 2 - Penerapan Kerangka Dasar (Aktif)
   a. Pengamanan diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
   b. Proses pengamanan informasi berjalan tanpa dokumentasi atau rekaman resmi.
   c. Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
   d. Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.
4. Tingkat 3 - Terdefinisi dan Konsisten (Pro Aktif)
   a. Bentuk pengamanan yang berlaku sudah diterapkan secara konsisten dan terdokumentasi secara resmi.
   b. Efektivitas pengamanan dievaluasi secara berkala, walaupun belum melalui proses yang terstruktur.
   c. Kerangka kerja pengamanan sudah mematuhi ambang batas minimum standar atau persyaratan hukum terkait.
   d. Secara umum semua pihakyang terlibat menyadari tanggung jawab mereka dalam pengamanan informasi.

5. Tingkat 4 - Terkelola dan Terukur (Terkendali)
    a. Pengamanan diterapkan secara efektif sesuai dengan strategi manajemen risiko.
    b. Evaluasi (pengukuran) pencapaian sasaran pengamanan dilakukan secara rutin, formal dan terdokumentasi.
    c. Penerapan pengamanan teknis secara konsisten dievaluasi efektivitasnya.
    d. Kelemahan manajemen pengamanan informasi terdefinisi dengan baik dan secara konsisten ditindak lanjuti pembenahannya.
    e. Karyawan merupakan bagian yang tidak terpisahkan dari pelaksana pengamanan informasi.
6. Tingkat 5 - Optimal
    a. Pengamanan menyeluruh diterapkan secara berkelanjutan dan efektif melalui program pengelolaan risiko yang terstruktur.
    b. Pengamanan informasi dan manajemen risiko sudah terintegrasi dengan tugas pokok instansi.
    c. Kinerja pengamanan dievaluasi secara kontinyu, dengan analis parameter efektivitas kontrol, kajian akar permasalahan dan penerapan langkah untuk optimasi peningkatan kinerja.
    d. Target pencapaian program pengamanan informasi selalu dipantau, dievaluasi dan diperbaiki.
    e. Karyawan secara proaktif terlibat dalam peningkatan efektivitas pengamanan informasi.
7. Tingkat 6 - Di Luar Jangkauan
    a. Kontrol yang berada diluar jangkauan