BAB 2
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Pada tinjauan pustaka dalam penelitian ini, terdapat beberapa penelitian terkait dengan menggunakan indeks KAMI diantaranya adalah penelitian yang dilakukan oleh Endi Lastyono Putra dkk[3]. Penelitian ini membahas evaluasi keamanan informasi pada divisi *Network of Broadband* PT. Telekomunikasi Indonesia Tbk. berdasarkan indeks KAMI. Penelitian tersebut berjudul "Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI)". Penelitian ini dilakukan untuk mengevaluasi keamanan informasi pada divisi *Network of Broadband* Telkom kota Bandung, menganalisis kondisi terkini keamanan informasi perusahaan dan membantu perusahaan dengan membuat rekomendasi perbaikan terhadap keamanan informasi. Metodologi yang digunakan adalah indeks Keamanan Informasi (KAMI) yang ditujukan untuk menganalisa kelayakan dan efektifitas keamanan informasi. Hasil penelitian yang dicapai menunjukan hasil penilaian tingkat kepentingan dan peran TIK sebesar 44 dari 48, hasil keseluruhan dari penilaian ke 5 area indeks KAMI sebesar 582 dari 588 dan berada pada level V.

Peneliti lain oleh Irawan Afriyanto dkk , untuk mengetahui tingkat kematangan keamanan informasi di perguruan tinggi X dengan menggunakan indeks KAMI. Dalam penelitian ini menggunakan observasi dan wawancara berdasarkan satndar ISO/IEC 27001:2009. Hasil dari penelitian ini didapatkan bahwa tingkat kematangan keamanan informasi Perguruan Tinggi X berada pada level I+ s/d II+. Penilitian ini mengukur tingkat kematangan keamanan informasi dengan indeks KAMI yang mencakup peran TIK, Tata Kelola, resiko, dan kerangka kerja, aset, dan teknologi keamanan informasi.

Tabel 2.1 Penelitian Terkait Penggunaan indeks KAMI ISO/IEC 27001:2009

No	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1.	Endi Listiyono, dkk, 2014	Evaluasi Keamanan Informasi	Evaluasi dengan Indeks KAMI ISO/IEC 27001:2009 yang mencakup 5 area indeks KAMI	Peran TIK sebesar 44 dari 48, keseluruhan hasil analisis sebesar 582 dari 588 dan berada pada level V
2.	Irawan Afriyanto, 2015	Pengkuran tingkat kematangan dan keamanan informasi	Standar ISO/IEC 27001:2009 dengan pengukuran pada 5 area indeks KAMI	Hasil pengukuan tingkat kematangan keamanan informasi secara keseluruhan berada pada level I+ s/d II+

2.2 Standar Sistem Manajemen Keamanan Informasi (SMKI)

Pada 2005, *International Organization for Standarization* (ISO) atau Organisasi Internasioanl untuk Standarisasi telah menjabarkan standar-standar mengenai *Information Security Management Systems* (ISMS) atau Sistem Manajamen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan.

Dari standar seri ISO 27000 ini hingga September 2011, baru ISO/IEC 27001:2005 yang telah diadopsi oleh Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) yang bernomor SNI ISO/IEC 2007:2009.

2.2.1 Kemanan Informasi

Menurut ISO/IEC 27001:2009 keamanan informasi adalah penjagaan kerahasiaan, identitas dan ketersediaan informasi. Keamanan informasi juga merupakan suatu bentuk usaha yang dilakukan untuk mengamankan informasi atau aset informasi yang dilakukan dengan berbagai upaya dengan tujuan untuk membuat aman suatu informasi yang ada [4]. Keamanan informasi berbeda dengan keamanan teknologi informasi atau *IT Security* akan tetapi, kedua hal tersebut saling terkait. Keamanan teknologi informasi mencakup kegiatan atau usaha-usaha pengamanan infrasruktur TI dari ancaman-ancaman yang berupa akses serta penggunaan jaringan tanpa seizin pihak yang berwenang, sementara keamanan informasi hanya mengacu pada data informasi milik organisasi atau perusahaan. Dalam hal ini usaha yang perlu dilakukan adalah mengembangkan, merencanakan, serta memantau semua kegiatan yang terkait dengan usaha untuk memebuat data dan informasi tersebut dapat berguna sesuai dengan fungsinya serta tidak disalahkan gunakan atau dibocorkan kepada pihak-pihak yanng tidak berwenang [2] . Berdasarkan hal tersebut maka teknologi informasi merupakan salah satu aset penting yang digunakan untuk mengamankan akses serta penggunaan data dan informasi yang dimiliki perusahaan. Dalam suatu organisasi keamanan informasi adalah aspek yang sangat penting , semakin banyak data dan informasi yang ada dalam organisasi tersebut maka semakin banyak ancaman keamanan informasi yang didapat oleh organisasi tersebut. Terdapat 5 layanan jaminan keamanan informasi, diantaranya adalah sebagai berikut [5]:

1. *Confidentiality*, yaitu memastikan terhadap pengaksesan informasi diakses hanya dapat dilakukan oleh pihak yang berkepentingan.
2. *Authenticity*, yaitu penjaminanan atas keaslian informasi.
3. *Integrity*, yaitu Pemastian akan ketepatan dan kelenggkapan informasi sesuai dengan bentuk semula.
4. *Availability*, yaitu memastikan bahwa orang yang berwenanglah yang hanya dapat mengakses suatu informasi dengan tepat waktu apabila data diperlukan.

5. *Non-Repudiation*, yaitu menjamin bahwa pihak pengguna tidak dapat menyangkal keaslian tanda tangan digital (digital signature) pada suatu dokumen atau tempat dalam suatu jaringan.

2.2.2 Sasaran Pengendalian Keamanan Informasi

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi yang diadopsi dari ISO 27001:2005, terdapat sebelas sasaran pengendalian yaitu sebagai berikut [2] :

1. Pengendalian Umum

   Sasaran ini digunakan sebagai acuan dalam kegiatan perlindungan aset informasi dalam lingkungan Kementrian Keuangan dari segala macam bentuk ancaman atau gangguan dari lingkungan internal maupun eksternal dan secara sengaja maupun tidak sengaja. Sasaran pengendalian ini mencakup pengelolaan keamanan seluruh aset informasi yang dilakukan oleh seluruh unit kerja, pegawai Kementrian Keuangan baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK), serta pihak ketiga di lingkungan Kementrian Keuangan.
2. Pengendalian Organisasi Keamanan Informasi

   Tujuan dari sasaran pengendalian ini yaitu untuk memberikan pedoman dalam suatu pembentukan organisasi yang fungsional dalam konteks keamanan informasi dan bertanggung jawab dalam pengelolaan keamanan informasi termasuk hubungannya dengan pihak luar.
3. Pengendalian Pengelolaan Aset

   Tujuan dari sasaran pengendalian ini yaitu untuk memberikan acuan dalam hal pengelolaan aset informasi guna melindungi dan menjamin keamanan aset informasi.
4. Pengendalian Keamanan Sumber Daya Manusia

   Tujuan dari sasaran pengendalian ini yaitu untuk memastikan bahwa seluruh pegawai maupun pihak ketiga mengerti dan memahami akan tanggung jawab masing-masing mengenai ancaman keamanan informasi serat memahami

semua proses yang berhubungan dengan keamanan informasi sebelum, selama dan sesudah bertugas.

5. Pengendalian Keamanan Fisik dan Lingkungan

   Tujuan dari sasarn pengendalian ini adalah untuk mencegah adanya akses fisik yang dilakukan oleh pihak yang tidak berwenang, serta menghindari terjadinya kerusakan pada perangkat pengolah informasi dan gangguan terhadap aktifitas organisasi.

6. Pengendalian Pengelolaan Komunikasi dan Operasi

   Tujuan dari sasaran ini adalah untuk memastikan bahwa perangkat operasional yang ada aman dan benar terhadap pengolahan informasinya. Tujuan lain dari sasaran ini adalah untuk mengimplementasikan, memelihara keamanan informasi, meminimalkan segala resiko kegagalan, memastikan akan keutuhan dan ketersediaan informasi, memastikan keamanan pertukaran informasi dan pemantauan proses operasional.

7. Pengendalian Akses

   Tujuan dari sasaran pengendalian ini adalah untuk memastikan otorisasi akses pengguna dan melakukan pencegahan terhadap akses oleh pihak yang tidak berwenang pada aset informasi khususnya pada perangkat pengolah informasi.

8. Pengendalian Pengadaan, Pengembangan, dan Pemeliharaan Sistem

   Tujuan dari sasaran pengendalian ini adalah untuk memastikan bahwa keamanan informasi merupakan bagian yang telah terintegrasi dengan sistem informasi, melakukan pencegahan akan terjadinya kesalahan, kehilangan serta modifikasi atau pengubahan oleh pihak-pihak yang tidak bertanggung jawab.

9. Pengendalian Pengelolaan Gangguan Keamanan Informasi

   Tujuan sasaran pengendalian ini adalah untuk memastikan kejadian dan kelemahan informasi yang terhubung dengan sistem informasi agar dapat dikomunikasikan dan dilakukan perbaikan, serta dilakukannya suatu pendekatan yang konsisten agar tidak terulang kembali kesalahan yang serupa.

10. Pengendalian Pengelolaan Kelangsungan Kegiatan

Tujuan dari sasaran pengendalian ini untuk melindungi sistem informasi, memastikan keberlangsungan kegiatan pada saat keadaan darurat dan untuk memastikan bahwa telah dilakukan pemulihan yang tepat.

11. Pengendalian Kepatuhan

    Sasaran pengendalian ini bertujuan untuk menghindari terjadinya pelanggaran terhadap peraturan perundang-undangan yang terkait keamanan informasi.

2.3 SNI ISO/IEC 27001:2009

ISO/IEC 27001 yang diciptakan pada 2005, merupakan Organisasi Internasional untuk Standarisasi (International Organization for Standarization) yang kemudianpada tahun 2011 telah diadopsi oleh Badan Standarisasi Nasional (BAN) sebagai Standar Nasional Indonesia (SNI) dengan berbahasa Indonesia yang bernomor SNI ISO/IEC 27001:2009. SNI ISO/IEC 27001:2009 ini, berisi karakteristik ketentuan yang harus patuhi untuk membangun sebuah Sistem Manajemen Keamanan Informasi (SMKI). Standar ini mempunyai sifat standar tersendiri atau khusus terhadap produk teknologi informasi dengan mensyaratkan penggunaan pendekatan manajemen berbasis risiko, serta dirancang untuk memastikan bahwa kontrol-kontrol keamanan yang telah dipilih mampu untuk menjaga aset informasi dari adanya berbagai resiko dan memberi keyakinan akan tingkat keamanan bagi pihak yang berkepentingan. Pengembangan standar ini dilakukan melalui pendekatan proses sebagai suatu model bagi penerapan, penetapan, pemantauan, pengoperasian, peninjauan ulang (*review*), pemeliharaan dan peningkatan suatu SMKI [4]. SMKI (Sistem Informasi Manajemen Keamanan Informasi) adalah suatu bentuk susunan proses yang dibuat berdasarkan pendekatan resiko bisnis untuk merencanakan (*plan*), mengimplementasikan dan mengoperasikan (*do*), memonitoring dan meninjau (*check*), serta memelihara dan meningkatkan atau mengembangkan (*act*) terhadap keamanan informasi perusahaan. Dalam menerapkan keamanan informasi aspek SMKI dan teknologi keamanan informasi tidak dapat dipisahkan. Artinya suatu organisasi tidak hanya menerapkan teknologi keamanan informasi saja tanpa menerapkan SMKI. Model *PLAN-DO-CHECK-ACT* (PDCA) diterapkan terhadap struktur keseluruhan proses

SMKI, dalam model PDCA keseluruhan proses SMKI dapat dilihat dalam tabel berikut [6] :

Tabel 2.2 Peta PDCA dalam Proses SMKI [4]

Model	Keseluruhan Proses
PLAN (Menetapkan SMKI)	Menyusun aturan SMKI , target, proses, dan prosedur yang relevan dalam pengelolaan resiko dan meningkatkan keamanan informasi agar memberikan hasil yang diharapkan .
DO (Menerapkan dan mengoperasikan SMKI)	Menggunakan dan mengoperasikan panduan SMKI, kontrol, proses, dan prosedur-prosedur.
CHECK (Memantau dan melakukan tinjau ulang SMKI)	Menelaah dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya .
ACT (Memelihara dan meningkatkan SMKI)	Merencanakan kegiatan perbaikan dan pencegahan, terhadap hasil evaluasi, audit internal dan tinjauan, manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

2.4 Indeks Keamanan Informasi (KAMI)

Indeks Keamanan Informasi (KAMI) yaitu suatu model evaluasi yang bertujuan untuk menganalisa tingkat kesiapan atau tingkat kelengkapan keamanan informasi di dalam suatu instansi pemerintah. Tujuan dari model evaluasi ini adalah untuk mendefinisikan suatu kondisi kesiapan yang meliputi kelengkapan dan

kematangan kepada pimpinan instansi yang berupa kerangka kerja keamanan informasi dan tidak bertujuan untuk menganalisa kelayakan atau efektifitas bentuk-bentuk pengamanan yang ada. Evaluasi dilakukan pada cakupan area yang menjadi sasaran dalam penerapan keamanan informasi dalam pembahasan yang telah memenuhi segala aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009.

Bentuk penerapan evaluasi dalam indeks KAMI disusun sehingga instansi pemerintah atau oragnisasi lain dapat menggunakannya, ukuran, maupun tingkat kepentingan penggunaan TIK dalam terwujudnya fungsi dan tugas pokok yang ada dalam instansi. Evaluasi ini menggunakan data yang kemudian diharapkan untuk dapat menghasilkan gambaran indeks kesiapan dari aspek kelengkapan hingga kematangan penerapan kerangka kerja keamanan informasi dapat difungsikan sebagai pembanding dalam rangka penyusunan langkah perbaikan dan prioritasnya [7]

2.5 Metode Penilaian Indeks KAMI

Penentuan dalam indeks KAMI meliputi keseluruhan komponen persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009, komponen ini disusun menjadi 5 area [4]:

1. Tata Kelola Informasi

   Tata kelola sebagai rumusan penerapan kontrol yang memiliki cakupan yang berupa kontrol umum organisasi, keamanan informasi dalam kegiatan pengelolaan kelangsungan usaha dan kepatuhan. Di dalam area ini sudah didefinisikan kesiapan bentuk tata kelola dalam aspek keamanan informasi beserta Instansi/fungsi, tugas, dan tanggung jawab pengelola keamanan informasi.
2. Pengelolaan Resiko Keamanan Informasi

   Penerapan kontrol dalam area ini yaitu sasaran pengendalian organisasi, pengelolaan aset informasi, keamanan informasi dalam pengelolaan kelangsungan usaha dan kepatuhan. Tujuan strategi dalam area pengelolaan resiko keamanan informasi adalah untuk memastikan teridentifikasinya

seluruh resiko dan terdapat mitigasi yang terencana dan terukur untuk menjaga agar resiko tersebut berada pada level yang telah ditetapkan.

3. Kerangka Kerja Keamanan Informasi

   Penerapan kontrol yang dilakukan dalam area ini yaitu sasaran pengendalian organisasi, keamanan pelaku (SDM), manajemen komunikasi dan standar operasionalnya, manajemen ancaman atau gangguan keamanan informasi. Kelengkapan kontrol dalam area ini adalah kebijakan prosedur kerja operasional, adanya persaingan antar sumber daya manusia termasuk strategi penerapan dan pengukuran efektifitas kontrol untuk menjalankan sasaran pembenahan. Area ini mengevaluasi kelengkapan dan kesiapan kerja (kebijakan dan prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

4. Pengelolaan Aset Informasi

   Rumusan penggunaan kontrol dalam mengelola aset informasi yaitu target pengendalian, keamanan sumber daya manusia, keamanan fisik dan lingkungan, pegendalian akses, dan keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi.

5. Teknologi dan Keamanan Informasi

   Rumusan penerapan kontrol pada area ini yaitu target pengendalian akses keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi, pengelolaan ancaman keamanan informasi dan pengelolaan kelangsungan usaha dan kepatuhan. Aspek dalam area ini mensyaratkan perlunya strategi yang berhubungan dengan tingkatan resiko.

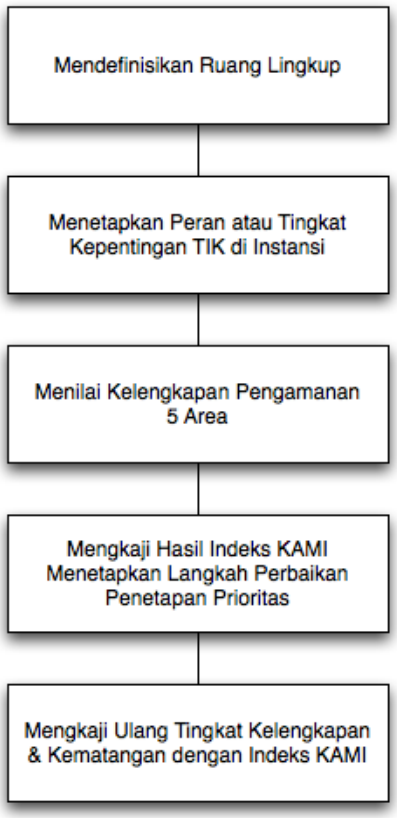
   Area ini untuk mengidentifikasi terhadap kelengkapan, konsisten dan evektivitas penggunaan teknologi dalam konsep pengamanan aset informasi.

Penyusunan 5 area ini dilakukan sebagai acuan pembanding dalam menyusun langkah perbaikan dan menetapkan prioritasnya, serta untuk membei kemudahan dalam evaluasi dimana hasil evaluasinya sendiri dapat dipergunakan sebagai acuan perbaikan dan peningkatan kinerja tata kelola keamanan informasi.

Terwujudnya pencapaian tujuan utama untuk pengamanan dalam setiap area membutuhkan evaluasi dari setiap aspek. Dalam tahapan penerapan pengamanan setiap memiliki karakteristik yang berbeda-beda sesuai dengan standar SNI ISO/IEC 27001:2009. Penyampaian konteks pertanyaan dari setiap aspek terdiri dari bentuk dasar kerangka kerja keamanan informasi, konsistensi penerapan, efektifitas, hingga kemampuan untuk selalu meningkatkan kinerja keamanan informasi [4].

2.6 Penggunaan Alat Evaluasi Indeks Keamanan Informasi

Gambaran proses indeks Kemanan Informasi seperti gambar berikut ini [4] :



Gambar 2.1 Ilustrasi Evaluasi

Ilustrasi diatas menjelaskan bahwa indeks KAMI merupakan seperangkat alat eavluasi yang digunakan dalam penggunaan tata kelola keamanan informasi yang dilakukan dengan berkelanjutan yang bertujuan untuk memberikan ilustrasi terhadap hasil dari penerapan tersebut. Terjadinya perubahan infrastruktur pada

kondisi awal evaluasi indeks KAMI, maka peninjauan ulang dilakukan untuk memberikan kepastian terhadap kematangan hasil evaluasi..

2.6.1 Penilaian Tingkat Kematangan

Definisi dari tingkat kematangan adalah untuk mengidentifikasi kelengkapan dan tingkat kematangan untuk penerapan pengamanan yang telah ditetapkan sebagai panduan di dalam indeks KAMI. SNI ISO/IEC 27001:2009 termasuk dalam penjabaran evaluasi kelengkapan yang bertujuan untuk menganalisa tingkat kematangan dengan pengelompokan proses yang terkait terhadap acuan dari *framework* COBIT atau CMMI. Hasil evaluasi nantinya dipergunakan sebagai pelaporan kesiapan keamanan informasi di Institusi/Lembaga Kementrian [4].

Tingkat kematangan yang di perlukan dalam indeks KAMI di kelompokkan sebagai berikut [2] :

1. Tingkat 0 – Dengan status “Tidak Diketahui (Pasif)”
    - Tidak diketahuinya status keamanan informasi.
    - Pihak-pihak yang terkait dalam konsep pengamanan informasi tidak mengikuti dan tidak melaporkan hasil tingkatan indeks KAMI.
2. Tingkat I – Dengan status “Kondisi Awal (Reaktif)”
    - Pemahaman terhadap pentingnya pengelolaan keamanan informasi mulai terlihat.
    - Penerapan dalam tingkat pengamanan masih bersifat tak beraturan, reaktif, tidak mengacu terhadap keseluruhan resiko dengan adanya jalur komunikasi tanpa pengawasan yang jelas.
    - Tidak teridentifikasinya kelemahan teknis dan non-teknis.
    - Tidak adanya kesadaran dan tanggung jawab dari pihak yang terlibat.
3. Tingkat II – Dengan status “Penerapan Kerangka Kerja Dasar (Aktif)”
    - Belum terwujudnya keterkaitan terhadap pengaman meskipun pengamanan sudah diterapkan dengan tujuan untuk mendapatkan strategi proses bisnis yang efektif.

- Tidak ada dokumentasi atau *file* rekaman resmi terhadap proses pengamanan.
- Prosedur operasional yang akan diterapkan masih bergantung terhadap pengetahuan dan kemauan diri dari setiap individu.
- Efektifitas bentuk keamanan informasi belum dapat dibuktikan secara menyeluruh.
- Masih sering ditemukan kelemahan dalam pengelolaan pengamanan dan belum dapat diselesaikan oleh unit pelaksana ataupun pimpinan sehingga memberikan akibat terhadap perubahan.
- Belum terdefinisikannya prioritas dalam pengelolaan keamanan
- Masih banyak pihak-pihak yang terlibat yang belum sepenuhnya memahami tanggung jawab masing-masing.

4. Tingkat III – Dengan kondisi "Terdefinisi dan Konsisten (Pro Aktif)"
    - Penerapan bentuk pengamanan sudah dilakukan dengan konsisten yang diikuti dengan pembuatan dokumentasi proses secara resmi
    - Dilakukannya evaluasi secara bertahap terhadap efektifitas pengelolaan keamanan.
    - Pimpinan dan pelaksana sudah dapat menangani apabila ditemukannya permasalahan yang terkait dengan pengelolaan keamanan, meskipun masih terdapat beberapa kelemahan.
    - Telah tercapainya ambang batas minimun kerangka kerja pengamanan.
    - Seluruh pihak sudah menyadari terhadap tanggung jawab pengelolaan masing-masing.
5. Tingkat IV – Dengan kondisi "Terkelola dan Terukur (Terkendali)"
    - Dilakukannya pengamanan yang efektif terhadap pengelolan resiko.
    - Dilakukan evaluasi dan pengukuran terhadap pencapaian tujuan pengamanan yang dilakukan dengan formal, bertahap dan terdokumentasi.
    - Dilakukan evaluasi secara rutin terhadap penerapan pengamanan teknis agar efektif.

- Telah teridentifikasinya kelemahan pengelolaan keamanan informasi secara terstruktur dan konsisten dalam penindaklanjutan perbaikannya.
- Pengelolaan pengamanan yang bersifat pro-aktif serta dilakukan penerapan perbaikan demi terwujudnya suatu bentuk lain dari pengelolaan secara efisien.
- Peristiwa terhadap ketidakpatuhan diselesaikan dengan proses formal dengan mengidentifikasi akar masalahnya.
- Karyawan adalah bagian yang penting dalam terlaksananya keamanan informasi.

6. Tingkat V – Status kondisi "Optimal (Optimal)"
   - Penerapan keseluruhan pengamanan dilakukan secara bertahap.
   - Terintegrasinya pengelolaan resiko dan pengelolaan keamanan informasi.
   - Dilakukan penilaian kinerja pengamanan secara berkelanjutan, yang mencakup analisis parameter efektifitas kontrol, bahasan akar permasalahan serta diterapkannya langkah-langkah dalam mengoptimalkan peningkatan kinerja.
   - Dalam melakukan peningkatan efektifitas keamanan informasi memerlukan tenanga karyawan yang pro-aktif.

2.6.2 Penetapan Sasaran Pengendalian

Untuk membangun suatu Sistem Manajemen Keamanan Informasi (SMKI) perlu dilakukannya penetapan sasaran pegendalian dan pengendalian sebagai langkah awal. Sasaran Pengendalian dan pengendalian tersebut telah didefinisikan dan diselaraskan dengan ISO/IEC 27001:2005 yang dimulai dari klausal 5 sampai klausal 15 [4] :

Tabel 2.3 Sasaran Pengendalian yang diselaraskan dengan ISO/IEC 27001:2005

No.	Klausal	Sub Klausal	Sasaran Pengendalian
1.	A.5		Sasaran Mengenai Kebijakan Keamanan
		a. A.5.1	Kebijakan terhadap Keamanan Informasi

		1). A.5.1.1	Dokumen mengenai kebijakan keamanan informasi
		2). A.5.2.1	Kajian terhadap kebijakan keamanan informasi
2.	A.6		Organisasi mengenai Keamanan Informasi
		a. A.6.1	Organisasi Internal
		1) A.6.1.1	Serangkaian komitmen manajemen terhadap suatu keamanan informasi
		2) A.6.1.2	Koordinasi mengenai keamanan informasi
		3) A.6.1.3	Alokasi tanggung jawab keamanan informasi
		4) A.6.1.4	Proses otorisasi untuk memfasilitasi pengolahan informasi
		5) A.6.1.5	Perjanjian perihal kerahasiaan
		6) A.6.1.6	Adanya kontak terhadap pihak yang berkepentingan
		7) A.6.1.7	Kontak terhadap suatu kelompok khusus (*special interest*)
		8) A.6.1.8	Kajian yang independen terhadap keamanan informasi
		b. A.6.2	Perihal pihak Eksternal
		1) A.6.2.1	Identifikasi resiko dari pihak eksternal
		2) A.6.2.2	Penekanan keamanan ketika menjalin kontak dengan pelanggan
		3) A.6.2.3	Penekanan perjanjian terhadap pihak ketiga
3.	A.7		Perihal Tanggung Jawab Terhadap Aset
		a. A.7.1	Tanggung Jawab Terhadap Aset
		1) A7.1.1	Inventaris aset
		2) A.7.2.2	Kepemilikan aset
		3) A.7.2.3	Penerapan aset yang telah masuk
		b. A.7.2	Klasifikasi Informasi

		1) A.7.2.1	Pedoman Klasifikasi
		2) A.7.2.2	Pelabelan dan penanganan informasi
4.	A.8		Keamanan Sumber Daya Manusia
		a. A.8.1	Sebelum dipekerjakan
		1) A.8.1.1	Tanggung jawab dan fungsi
		2) A.8.1.2	Penyaringan (*screening*)
		3). A.8.1.3	Rumusan syarat dan aturan dalam kepegawaian
		b. A.8.2	Selama Bekerja
		1) A.8.2.1	Tanggung jawab manajemen
		2) A.8.2.2	Pendidikan, kepedulian, dan pelatihan pada keamanan informasi
		3) A.8.2.3	Proses pendisiplinan
		c. A.8.3	Pengakhiran atau Perubahan Pekerjaan
		1) A.8.3.1	Tanggung jawab pengakhiran pekerjaan
		2) A.8.3.2	Pegembalian aset
		3) A.8.3.3	Penghaapusan hak akses
5.	A.9		
		a. A.9.1	Area yang Aman
		1) A.9.1.1	Parameter keamanan fisik
		2) A.9.1.2	Pengendalian entri yang bersifat fisik
		3) A.9.1.3	Menjaga ruangan, kantor, atau fasilitas lainnya
		4) A.9.1.4	Penjagaan terhadap adanya ancaman eksternal dari lingkungan
		5) A.9.1.5	Bekerja di area yang aman
		6) A.9.1.6	Area akses publik dan bongkar muat
		b. A.9.2	Keamanan Peralatan
		1) A.9.2.1	Penempatan dan perlindungan peralatan
		2) A.9.2.2	Sarana pendukung

		3) A.9.2.3	Keamanan kabel
		4) A.9.2.4	Pemeliharaan peralatan
		5) A.9.2.5	Keamanan peralatan diluar lokasi
		6) A.9.2.6	Pembuangan atas penggunaan kembali peralatan dengan aman
		7) A.9.2.7	Pemindahan barang
6.	A.10		Pengelolaan Komunikasi dan Operasi
		a. A.10.1	Prosedur Operasional dan Tanggung Jawab
		1) A.10.1.1	Prosedur operasi yang terdokumentasi
		2) A.10.1.2	Pengelolaan perubahan
		3) A.10.1.3	Pemisahan tugas
		4) A.10.1.4	Pemisahan fasilitas pengujian, pembangunan, dan operasional
		b. A.10.2	Manajemen dalam Pelayanan Jasa Pihak Ketiga
		1) A.10.2.1	Pelayanan jasa
		2) A.10.2.2	Pemantauan dan pengkajian jasa pihak ketiga
		3) A.10.2.3	Pengelolaan perubahan terhadap jasa pihak ketiga
		c. A.10.3	Perencanaan dan Penerimaan Sistem
		1) A.10.3.1	Pengelolaan kapasitas
		2) A.10.3.2	Keberterimaan sistem
		d. A.10.4	Perlindungan terhadap *malicious and mobile code*
		1) A.10.4.1	Pengendalian terhadap *malicious code*
		2) A.10.4.2	Pengendalian terhadap *mobile code*
		e. A.10.5	Back-up
		1) A.10.5.1	*Back-up* informasi
		f. A.10.6	Manajemen Keamanan Jaringan
		1) A.10.6.1	Pengendalian jaringan
		2) A.10.6.2	Keamanan layanan jaringan

		g. A.10.7	Penanganan Media
		1) A.10.7.1	Manajemen yang dapat dipindahkan
		2) A.10.7.2	Pemusnahan media
		3) A.10.7.3	Prosedur penanganan informasi
		4) A.10.7.4	Keamanan dokumentasi sistem
		h. A.10.8	Pertukaran Informasi
		1) A.10.8.1	Aturan dan prosedur perihal pertukaran informasi
		2) A.10.8.2	Perjanjian dalam pertukaran
		3) A.10.8.3	Media fisik dalam transit
		4) A.10.8.4	Pesan elektronik
		5) A.10.8.5	Sistem informasi bisnis
		i. A.10.9	Layanan *E-Commerce*
		1) A.10.9.1	*Electronic Commerce*
		2) A.10.9.2	Transaksi online
		3) A.10.9.3	Aspek Informasi yang tersedia untuk umum
		j. A.10.10	Pemantauan
		1) A.10.10.1	*Log audit*
		2) A.10.10.2	Pemantauan penggunaan sistem
		3) A.10.10.3	Perlindungan informasi *log*
		4) A.10.10.4	*Log* Adiminstrator dan operator
		5) A.10.10.5	*Log* pada kesalahan yang terjadi
		6) A.10.10.6	Sinkronisasi penunjuk waktu
7.	A.11		Pengendalian Akses
		a. A.11.1	Persyaratan proses bisnis dalam Pengendalian Akses
		1) A.11.1.1	Kebijakan pengendalian akses
		b. A.11.2	Manajemen Akses Pengguna
		1) A.11.2.1	Pendaftaran pengguna
		2) A.11.2.2	Pengelolaan hak khsusus
		3) A.11.2.3	Manajemen *password* pengguna

		4) A.11.2.4	Tinjauan terhadap hak akses pengguna
		c. A.11.3	Tanggung Jawab Pengguna
		1) A.11.3.1	Penggunaan *password*
		2) A.11.3.2	Peralatan yang telah ditinggalkan oleh penggunanya
		3) A.11.3.3	Kebijakan *clear desk* dan *clear screen*
		d. A.11.4	Pengendalian Akses Jaringan
		1) A.11.4.1	Kebijakan mengenai penggunaan layanan jaringan
		2) A.11.4.2	Otentikasi pengguna untuk koneksi eksternal
		3) A.11.4.3	Identifikasi peralatan dalam jaringan
		4) A.11.4.5	Perlindungan terhadap *remote diagnostic* dan *configuration port*
		5) A.11.4.6	Segregasi dalam jaringan
		6) A.11.4.7	Pengendalian koneksi jaringan
		7) A.11.4.8	Pengendalian *routing* jaringan
		e. A.11.5	Pengendalian Akses Sistem Operasi
		1) A.11.5.1	Langkah log-on yang aman
		2) A.11.5.2	Proses identifikasi dan otentikasi pengguna
		3) A.11.5.3	Sistem manajemen *password*
		4) A.11.5.4	Penggunaan *system utilities*
		5) A.11.5.5	Sesi *time-out*
		6) A.11.5.6	Pembatasan waktu koneksi
		f. A.11.6	Pengendalian Akses Aplikasi dan Informasi
		1) A.11.6.1	Pembatasan akses informasi
		2) A.11.6.2	Isolasi sistem yang sensitif
		g. A.11.7	*Mobile Computing* dan Kerja Jarak Jauh (*Teleworking*)
		1) A.11.7.1	*Mobile Computing* dan komunikasi
		2) A.11.7.2	Kerja jarak jauh

8.	A.12	a. A.12.1	Pengembangan, Pemeliharaan, dan Akuisisi Sistem Informasi
		1) A.12.1.1	Persyaratan Keamanan dari Sistem Informasi
		b. A.12.2	Pengolahan yang Benar dalam Aplikasi
		1) A.12.2.1	Validasi dan masukan
		2) A.12.2.2	Pengendalian pengolahan internal
		3) A.12.2.3	Integritas pesan
		4) A.12.2.4	Validasi dan keluaran
		c. A.12.3	Pengendalian dengan Cara Kriptografi
		1) A.12.3.1	Kebijakan tentang hal penggunaan pengendalian kriptografi
		2) A.12.3.2	Manajemen kunci
		d. A.12.4	Keamanan *System Files*
		1) A.12.4.1	Pengendalian terhadap perangkat lunak yang operasional
		2) A.12.4.2	Perlindungan data uji sistem
		3) A.12.4.3	Pengendalian akses terhadap kode sumber program
		e. A.12.5	Keamanan dalam Proses Pengembangan dan Pendukung
		1) A.12.5.1	Prosedur pengendalian perubahan
		2) A.12.5.2	Rumusan teknis berdasarkan aplikasi setelah perubahan sistem operasi
		3) A.12.5.3	Pembatasan mengenai perubahan terhadap paket perangkat lunak
		4) A.12.5.4	Kebocoran informasi
		5) A.12.5.5	Pengembangan perangkat lunak yang telah di alihdayakan
		f. A.12.6	Manajemen Kerawanan Teknis
		1) A.12.6.1	Pengendalian Kerawanan Teknis
9.	A.13		Manajemen Insiden Keamanan Informasi
		a. A.13.1	Melaporkan insiden dan Kelemahan

			dari Keamanan Informasi
		1) A.13.1.1	Melaporkan insiden terhadap keamanan informasi
		2) A.13.1.2	Pelaporan kelemahan keamanan
		b. A.13.2	Manajemen mengenai Insiden Keamanan Informasi dan perbaikan
		1) A.13.2.1	Tanggung jawab dan prosedur
		2) A.13.2.2	Pembelajaran dari insiden keamanan informasi
		3) A.13.2.3	Pengumpulan informasi
10.	A.14		Manajemen Keberlanjutan Bisnis (*Business Continuity Management*)
		a. A.14.1	Konsep Keamanan Informasi berdasarkan Manajemen Keberlanjutan Bisnis
		1) A.14.1.1	Memasukkan keamanan informasi ke dalam suatu proses manajemen keberlanjutan bisnis
		2) A.14.1.2	Keberlanjutan bisnis dan assesment resiko
		3) A.14.1.3	Pengembangan serta penerapan rencana keberlanjutan yang termasuk keamanan informasi
		4) A.14.1.4	Kerangka kerja perencanaan keberlanjutan bisnis
		5) A.14.1.5	Pengujian, pemeliharaan, dan assemen ulang rencana keberlanjutan bisnis
11.	A.15		Kesesuaian
		a. A.15.1	Kesesuaian dengan Persyaratan Hukum
		1) A.15.1.1	Identifikasi peraturan hukum yang berlaku
		2) A.15.1.2	Hak Kelayakan Intelektual (HAKI)
		3) A.15.1.3	Perlakuan pada perlindungan dokumentasi organisasi
		4) A.15.1.4	Perlakuan perlindungan data dan rahasia informasi pribadi

		5) A.15.1.5	Melakukan pencegahan penyalahgunaan fasilitas pengolahan informasi
		6) A.15.1.6	Disusunya regulasi pengendalian kriptografi
		b. A.15.2	Dilakukan pemenuhan terhadap standar Kebijakan Keamanan dan Pemenuhan Teknis
		1) A.15.2.1	Dilakukan pemenuhan terhadap standar kebijakan keamanan
		2) A.15.2.2	Dilakukan pengecekan pemenuhan teknis
		c. A.15.3	Pertimbangan Audit Sistem Informasi
		1) A.15.3.1	Dilakukan pengendalian audit sistem informasi
		2) A.15.3.2	Dilakukan perlindungan terhadap alat audit informsasi