Perancangan Sistem Keamanan Informasi Berbasis Penilaian Resiko Menggunakan ISO/IEC 27001 Dan ISO/IEC 27005 (Studi Kasus : Kajian Teoritis)

Suhana Minah Jaya
Prodi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Cirebon
suhanaminahjaya@umc.ac.id

Abstrak

Informasi merupakan sebuah aset penting dan bermanfaat bagi lancarnya roda bisnis suatu perusahaan atau organisasi. Didasari pentingnya informasi dan terjadinya bentuk kegagalan pada fungsi sistem informasi ini bermacam-macam, mulai dari gangguan dan putusnya jaringan, kerusakan hardware, gangguan software, gangguan pada aset sarana pendukung seperti hilangnya catu daya listrik, rusaknya AC, serangan hacker, virus, pencurian data, denial of services attack (DOS) pada Sistem Informasi Manajemen akademik sehingga perlu diterapkannya pengamanan terhadap aset informasi.

Dalam penelitian ini dibangun perancangan sistem manajemen keamanan informasi (SMKI) sebagai langkah awal organisasi untuk mengamankan informasi dari gangguan maupun ancaman baik dari dalam maupun dari luar perusahaan atau organisasi.

Dalam perancangan sistem keamanan informasi langkah-langkah yang dilakukan berdasarkan pada penilaian risiko dengan standar ISO 27005 yang terdiri dari identifikasi aset, identifikasi kerentanan, ancaman, konsekuensi, dan dampak yang selanjutnya dilakukan analisis risiko. Hasil dari analisis risiko kemudian menentukan kontrol objek dan kontrol keamanan menurut standar ISO/IEC 27001 berdasarkan risiko-risiko yang dimitigasi dari hasil analisis risiko.

Berdasarkan peneltian didapat sejumlah risiko-risiko yang harus dimitigasi. Untuk mengatasinya maka dipilih klausa 8, 9, 11 dan 12 yang terdiri dari kontrol keamanan dan klausa-klausa tersebut bisa mengatasi risiko-risiko yang dimitigasi untuk mendukung penerapaan sistem keamanan informasi. Kebijakan-kebijakan yang telah ditentukan kemudian dijabarkan berupa dokumentasi SMKI. Dokumentasi ini digunakan sebagai acuan berupa (*checklist*) kontrol meliputi Pedoman/manual mutu, Prosedur mutu, Instruksi kerja, dan Formulir, berdasarkan ISO/IEC 27001 untuk pengamanan informasi. SMKI juga menawarkan pemilihan kendali keamanan sebagai usaha perlindungan terhadap ancaman risiko dari proses dan aset.

Kata Kunci : Informasi, sistem manajemen keamanan informasi, analisis risiko ISO/IEC 27005, kontrol keamanan ISO/IEC 27001.

1. Pendahuluan

Keamanan informasi berkaitan dengan perlindungan asset berharga terhadap kehilangan, pengungkapan penyalahgu naan, atau kerusakan. Dalam konteks ini, "aset berharga" adalah informasi yang direkam, diproses, disimpan, dikirim atau diambil baik dari media elektronik atau non-elektronik. Upaya perlindungan terse but dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis **[17]**

Organisasi keamanan informasi memiliki tiga aspek yang harus dipahami untuk bisa menerapkannya, aspek tersebut biasa disebut dengan CIA Triad Model, yang antara lain adalah **[9]** :

1. *Confidentiality* (kerahasiaan). Merupakan aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang.
2. *Integrity* (integritas). Merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menajaga keakuratan dan keutuhan informasi.
3. *Availability* (ketersediaan). Menurut Peltier, T.

R., (2001), bahwa aspek keamanan informasi dapat digambarkan sebagai mana tampak pada gambar di bawah ini. [14].

Gambar 2.1 : *Aspek Keamanan Informasi*

Selain aspek di atas, keamanan informasi dapat juga diklasifikasikan sebagai berikut [20]:

1. *Physical Security* (keamanan fisik) merupakan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. *Personal Security* (keamanan pribadi) merupakan bagian dari keamanan fisik yang melindungi sumber daya manusia dalam organisasi atau pengguna yang memiliki akses terhadap informasi.
3. *Operation Security* (keamanan operasional) yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
4. *Communications Security* (Keamanan Komunikasi) yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.

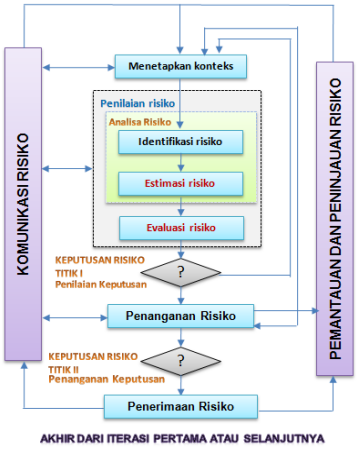
2.2 Teori Khusus

2.2.1 Manajemen Risiko

Risiko adalah sesuatu yang terjadi akibat adanya kelemahan pada aset yang menimbulkan ancaman dalam kurun waktu tertentu (probabilitas) serta memberikan dampak kepada organisasi. Manajemen risiko adalah suatu proses yang digunakan oleh suatu organisasi dalam mengidentifikasi, mengukur, mengawasi, dan meminimalkan pengaruh yang merugikan dari suatu risiko dengan mengidentifikasi, memantau, mengevaluasi, dan mengendalikan risiko tersebut dan menerapkan sebuah metode pengendalian yang efektif. Di dalam penerapan Sistem Keamanan Informasi, manajemen risiko merupakan salah satu bagian penting karena dengan melakukan manajemen risiko, bisa diketahui secara jelas apa saja aset yang harus dilindungi, ancaman apa saja yang mungkin terjadi, gambaran seberapa besar dampak yang mungkin terjadi, dan bagaimana proteksi terhadap aset yang harus diberikan. Sehingga Sistem Keamanan Informasi yang diterapkan dalam organisasi dapat dilakukan secara efektif.

2.2.1.1 ISO 27005

ISO 27005 adalah anggota keluarga standar ISO 27000 yang berfokus pada penilaian dan penanganan risiko. Standar ini mendukung konsep SMKI dalam standar ISO 27001 jika dilakukan dengan pendekatan manajemen risiko[6]. Untuk mengerti cara penerapan standar ini diharapkan mengerti konsep SMKI dengan ISO 27001 atau ISO 27002. Ada delapan proses yang dilakukan untuk melakukan manajemen risiko yang digambarkan sebagai berikut [6]:



Gambar 2.2 : *Proses Manajemen Risiko Keamanan Informasi*
(Sumber : BSNI ISO 27005 : 2009)

Sebagaimana yang terdapat Pada gambar 2.4 menggambarkan secara garis besar langkah-langkah

manajemen risiko guna keamanan informasi berdasarkan ISO/IEC 27005 dan secara umum manajemen risiko memang bertujuan untuk melihat dan mengkaji risiko secara menyeluruh dan merupakan salah satu yang dapat digunakan dalam manajemen risiko.

Jika standar ini diterapkan dalam penerapan SMKI dengan ISO 27001 maka akan dibagi menjadi beberapa tahap sebagai berikut [6]:

2.2.1.1.1 Komunikasi Risiko

Kesuksesan penilaian risiko tergantung pada efektifitas komunikasi dan konsultasi dengan para stakeholder. Keterbatasan pada penelitian ini adalah bahwa data dan informasi mengenai proses, input dan aktifitas didapat dari website Ditjen Pajak tanpa ada komunikasi dan konsultasi langsung dengan stakeholders.

2.2.1.1.2 Menetapkan konteks.

Masukan dari proses ini adalah seluruh informasi dari organisasi yang relevan dengan manajemen risiko. Ini menjadi bagian yang sangat mempengaruhi tujuan dari seluruh proses manajemen risiko. Cakupan dari manajemen risiko harus ditetapkan dan memenuhi seluruh aset yang dianalisis pada penilaian risiko.

2.2.1.1.3 Penilaian Risiko.

Penilaian risko dipakai untuk menentukan nilai dari aset informasi, mengidentifikasi ancaman dan kerentanan yang bisa terjadi, mengidentifikasi kontrol dan pengaruhnya terhadap sistem, menentukan besar konsekuensi yang ditimbulkan, dan pada akhirnya memprioritaskan risiko-risiko yang kemungkinan terjadi. Penilaian risiko terbagi menjadi dua proses, yaitu :

a. Analisis risiko.

Analisis risiko dibagi ke dalam dua proses sebagai berikut :

i. Identifikasi risiko.

Tujuan dari identifikasi risiko adalah untuk menentukan besar kemungkinan kerusakan dan mendapatkan informasi bagaimana, dimana, dan mengapa kerusakan tersebut bisa terjadi. Pada tahap identifikasi risiko ini akan dilakukan identifikasi aset, ancaman, kontrol yang digunakan, kerentanan, dan konsekuensi.

ii. Estimasi risiko.

Estimasi risiko dapat dilakukan secara kuantitatif ataupun kualitatif. Estimasi kuantitatif menggunakan skala dengan angka untuk menentukan beberapa besar konsekuensi dan kemungkinan terjadi sebuah risiko dengan menggunakan data dari beberapa sumber. Sementara estimasi kualitatif menggunakan skala kualitatif untuk mendeskripsikan besar kemungkinan dan konsekuensi dari sebuah risiko. Dan secara umum estimasi risiko kualititatif lebih mudah dimengerti saat kerugian bergantung secara subjektif pemilihan skala. Pada estimasi risiko dilakukan penilaian konsekuensi, penilaian kemungkinan, dan ditentukan tingkat dari estimasi risiko.

b. Evaluasi risiko.

Evaluasi risiko dipakai sebagai bahan untuk mengambil keputusan yang harus secara konsisten sesuai dengan konteks manajemen risiko baik secara eksternal maupun internal. Keputusan yang diambil dalam evaluasi risiko adalah berdasarkan persetujuan akan tingkat risiko pada proses sebelumnya. Namun, konsekuensi, kemungkinan, dan tingkat kepercayaan pada identifikasi dan analisis risiko harus diyakinkan secara baik.

2.2.1.1.4 Penanganan Risiko.

Ada empat penanganan terhadap risiko setelah berhasil diidentifikasi, yaitu sebagai berikut :

1. Penghindaran risiko (*risk avoidance*)

Penghindaran risiko berarti tidak melakukan aktivitas apapun yang memungkinkan datangnya risiko. Menghindari semua risiko berarti membatasi seluruh fungsionalitas sistem atau menghindari timbulnya biaya tambahan bila risiko diterima.

2. Pengurangan Risiko (*risk reduction*)

Pengurangan risiko adalah perlakuan yang mencakup metode yang diambil untuk mengurangi keparahan akibat suatu insiden. Contoh pengurangan risiko antara lain penggunaan pengendalian internal yang efektif, penggunaan firewall dan intruder detection systems (IDSs) untuk mengurangi kemungkinan serangan terhadap kerentanan, atau simplifikasi proses bisnis yang dapat mengurangi risiko atau mengurangi biaya.

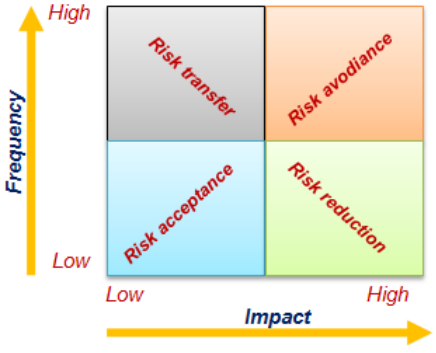
3. **Pengalihan Risiko *(risk transfer)***

   Pengalihan risiko berarti mengalihkan risiko ke pihak lain. Contoh pengalihan risiko adalah asuransi.

4. **Penerimaan Risiko *(risk acceptance)***

   Penerimaan risiko adalah perlakuan dimana risiko dari insiden dapat diterima. Penerimaan terhadap suatu risiko dapat menjadi layak ketika dampak atau kemungkinannya kecil, atau biaya untuk menanggulanginya lebih kecil dari kemungkinan dampak yang dihasilkan. Risiko yang tidak semuanya dihindari, dikurangi, atau dialihkan merupakan bagian dari penerimaan risiko.

   Pilihan perlakuan atas risiko terkait dengan frekuensi dan dampaknya tersebut dapat dilihat pada gambar berikut.



Gambar 2.3 : *Pilihan perlakuan risiko (Jones, 2007)*

2.2.2 Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan informasi (SMKI) merupakan sebuah kesatuan system yang disusun berdasarkan pendekatan resiko bisnis, untuk pengembangan, implementasi, pengoperasian, pengawasan, pemeliharaan serta peningkatan keamaan informasi perusahaan.

Sistem Manajemen Keamanan Informasi (SMKI) diterapkan dengan menggunakan model Plan Do Check Act (PDCA) . Tahapan dalam model tersebut adalah sebagai berikut [8]:

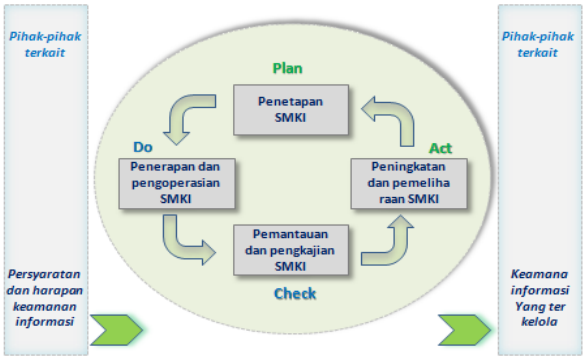
1 PLAN (Established SMKI) ; Tahap penyusunan rencana yang akan dilakukan, penentuan masalah yang akan diatasi, kelemahan yang akan diperbaiki serta pencarian solusi untuk mengatasi masalah.

2. DO (implement and operate the SMKI) ; Tahap dimana solusi dan perubahan dari proses yang telah direncanakan dilaksanakan. Dengan penerapan prosedur-prosedur serta instruksi kerja sesuai dengan aktivitas yang terjadi dalam organisasi.

3. Check (monitor and review the SMKI) ; Tahapan untuk meneliti apa yang telah dilaksanakan dan menemukan kelemahan-kelemahan yang perlu diperbaiki. Berdasarkan kelemahan-kelemahan tersebut kemudian disusun rencana perbaikan.

4. ACT (maintain and improve the SMKI) ; Tahap ini adalah usaha perbaikan berdasarkan hasil perubahan, meliputi pengambilan langkah korektif dan preventif berdasarkan hasil dari audit internal SMKI, tinjauan manajemen atau informasi lain yang relevan.

Proses yang didefinisikan dalam ISO/IEC 27001 dalam membangun SMKI mengadopsi siklus PDCA. Penjelasan PDCA yang diaplikasikan pada SMKI adalah sebagai berikut [8] :



Gambar 2.4 : *Pemetaan SMKI terhadap model PDCA*
(Sumber : *ISO / IEC 27001 : 2005*)

Model **Plan - Do - Check - Act (PDCA)** diterapkan terhadap struktur keseluruhan proses SMKI. Dalam model PDCA, keseluruhan proses SMKI dapat dipetakan seperti **Tabel 2.1**.

Standar menyatakan persyaratan utama yang harus dipenuhi menyangkut :

- Sistem manajemen keamanan informasi (kerangka kerja, proses dan dokumentasi)
- Tanggung jawab manajemen

Tabel 2.1: Peta PDCA dalam proses SMKI

Proses SMKI	Proses Manajemen Risiko Keamanan informasi
Plan (Perencanaan)	Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola resiko dan meningkatkan keamanan informasi agar memberi-kan hasil sesuai dengan keseluruhan kebijakan dari sasaran
Do (menerapkan dan mengoperasi kan SMKI)	Menetapkan dan mengoperasikan kebijakan SMKI
Check(memantau dan melakukan tinjau ulang SMKI)	Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya
ACT (memelihara dan meningkat kan SMKI)	Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatkan yang berkelanjutan.

(**Sumber :** *ISO/IEC 27001: 2005*)

2.2.2.1 ISO/IEC 27001

ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi**[7]** di perusahaan. Sarno dan Iffano (2009: 187) mengatakan kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol keamanan (*security control clauses*), 39 objektif kontrol (*control objectives*) dan 133 kontrol keamanan/kontrol (*controls*).

3. METODE PENELITIAN

Metode penelitian yang digunakan oleh penulis dalam pembuatan tesis ini adalah menggunakan metode deskriptif. Berikut adalah tahap-tahap dari metode penelitian yang dilakukan.

3.1. Studi Literatur

Studi literatur adalah tahap untuk mencari referensi data dan teori yang relevan dengan kasus atau permasalahan yang penulis teliti. Referensi yang diacu adalah sebagai berikut:

- Jurnal sebagai sumber data (Perancangan Sistem Manajemen Sekuritas Informasi (SMSI) Berdasarkan ISO/IEC 27001 Studi Kasus: Program Magister Manajemen Teknologi (MMT-ITS))
- Manajemen Risiko Keamanan Informasi ISO/IEC 27005.
- Sistem Manajemen Keamanan Informasi ISO/IEC 27001 dan ISO/IEC 27002.

3.3.1 Penilaian Risiko

Langkah awal dari tahapan Manajemen Risiko adalah Penilaian Risiko. Penilaian risiko menentukan nilai aset informasi, mengidentifikasi ancaman dan kerentanan yang berlaku yang telah ada (atau bisa ada). mengidentifikasi kontrol yang ada dan efeknya pada risiko yang teridentifikasi, menentukan konsekuensi potensial dan akhirnya memprioritaskan risiko yang diperoleh dan peringkat mereka terhadap kriteria evaluasi resiko y ang ditetapkan dalam pembentukan konteks.

3.3.1.1 Analisis Risiko

Analisis risiko sebagai proses penilaian terhadap risiko yang telah teridentikasi dalam rangka mengestimasi kemungkinan munculnya dan besaran dampak untuk menetapkan level atau status risikonya. Status risiko ditentukan berdasarkan kombinasi antara kemungkinan (probabilitas/ frekuensi) terjadnya risiko dan dampak (efek) jika risiko terjadi.

Langkah-langkah analisa risiko tersebut adalah sebagai berikut :

Tabel 3.1 Penilaian Kualitatif Kemungkinan/Frekuensi

Tingkat Kemungkinan		Deskripsi
1	Langka terjadi	Kemungkinan terjadi dalam rentang waktu 6-10 Tahun
2	Jarang terjadi	Kemungkinan terjadi dalam rentang waktu 1-5
3	Cukup sering terjadi	Akan terjadi setidaknya satu kali per tahun
4	Sering terjadi	Akan terjadi setidaknya satu kali per bulan
5	Sangat sering terjadi	Akan terjadi setidaknya satu kali per minggu

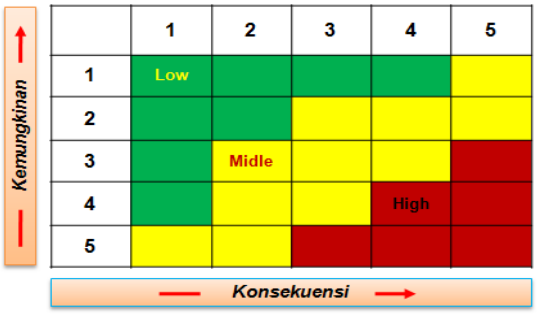
Selanjutnya penilaian terha dap dampak yang dihasilkan bagi perusahaan akan ditunjukkan Tabel 3.2 berikut ini. Dampak diklasifikasi kan berdasarkan beberapa parame ter seperti operasional, kinerja, reputasi dan finansial.

Tabel 3.2 Penilaian dampak risiko

Tingkat Dampak	Operasional	Kinerja	Reputasi	Finansial
1	Tidak menimbulkan penundaan aktivitas	Tidak terja di gangguan pada proses layanan	Tidak ada Publikasi	Kerugian atau biaya yang harus dikeluarkan di bawah Rp 1.000.000
2	Menimbulkan penundaan aktivitas (proses tidak dapat dijalankan) maksimum se lama 1 hari	Menimbulkan gangguan kecil Pada proses layanan namun tidak signifikan	Terdapat citra negatif namun tidak mengakibatkan penurunan kepercayaan	Kerugian atau biaya yang harus dikeluarkan Rp 10.000.000 hingga Rp1.000.001
3	Menimbulkan penundaan aktivitas (proses tidak dapat dijalankan) Maksimum selama 2 hari	Menimbulkan gangguan kegiatan pada kegiatan operasional layanan pendukung	Pemberitaan negatif yang menurunkan kepercayaan Stakeholders	Kerugian atau biaya yang harus dikeluarkan Rp 10.000.001 hingga Rp 50.000.000,-
4	Menimbulkan penundaan aktivitas (proses tidak dapat dijalankan) maksimum selama 3 hari	Menimbulkan gangguan kegiatan pada kegiatan operasional layanan utama	Pemberitaan negatif yang menurunkan kepercayaan Stakeholders	Kerugian atau biaya yang harus dikeluarkan Rp 50.000.001 hingga Rp 100.000.000
5	Menimbulkan penundaan aktivitas (proses tidak dapat dijalankan) lebih dari 3 hari	Menimbulkan gangguan kegiatan operasional layanan pendukung dan layanan utama	Hilang kepercayaan Stakeholders	Kerugian atau biaya yang harus dikeluarkan lebih dari Rp 100.000.000

Setelah penentuan nilai ancaman dan kerawanan dari tiap risiko diidentifikasi, maka selanjutnya dilakukan perhitungan nilai risiko. Penilaian risiko dilakukan dengan dengan mengalikan nilai kecenderungan yang sudah teridentifikasi sebelumnya dengan berapa besar dampak yang dihasilkan bagi perusahaan. Pada Tabel 3.3 berikut ini akan disajikan matriks penilaian dari nilai risiko dasar.

Tabel 3.3 Matriks analisis risiko dasar



Berdasarkan hasil penilaian risiko yang didapatkan dari proses identifikasi dan analisis risiko pada Tabel 3.3 selanjutnya dilakukan beberapa tindakan yang diperlukan seperti ditunjukkan pada Tabel 3.4 berikut. Apabila nilai risiko "Sedang" atau "Tinggi" maka jenis pengendalian adalah "Kontrol" atau dibutuhkan kontrol tambahan untuk meminimalisir risiko.

Tabel 3.4. *Nilai Pengendalian*

Nilai/Warna	Kriteria Pengendalian	Keterangan
1	Low	Pelaksanaan kontrol tidak berjalan baik dan tidak dimonitor sehingga tidak mempengaruhi tingkat risiko
2	Medium	Pelaksanaan kontrol ti dak berjalan konsisten dan terjadi berulang kembali sehingga tidak sepenuh nya mampu me ngurangi atau memini malkan tingkat risiko
3	Strong	Penerapan kontrol sudah cukup baik dan konsisten sehingga dapat mengu rangi/meminimalkan tingkat risiko.

Selanjutnya untuk mencari nilai risiko akhir digunakan matriks dengan parameter dari nilai risiko dasar dan nilai pengendalian seperti pada Tabel 3.5 berikut ini:

Tabel 3.5. *Nilai Pengendalian*

		Nilai Risiko Dasar		
		Low	**Medium**	**High**
Nilai Pengendalian	**Low**	Medium	Medium	High
	Medium	Low	Sedang	High
	Strong	Low	Low	Medium

Setelah melakukan identifikasi ancaman, setiap ancaman akan diberi nilai sesuai dengan kriteria yang ditentukan. Nilai diberikan masih secara kualitatif yang dikemudian akan diberian bobot nilai secara kuantitatif pada tahap analisis risiko. Penilaian ancaman ini juga akan mempengaruhi dalam mengambil keputusan perlakuan risiko. Kriteria penilaian ini tidak memiliki standar atau ketentuan tertentu tetapi sebaiknya ditetapkan dengan pengklasifikasian yang mudah dimengerti dan disetujui oleh manajemen keamanan informasi organisasi. Adapun kriteria yang dipakai dalam melakukan penilaian ancaman adalah sebagai berikut :

Tabel 3.6 Kriteria Penilaian Ancaman

Kriteria Kekuatan Ancaman	Deskripsi
Low (L)	Ancaman tidak mempengaruhi operasi bisnis.
Medium (M)	Ancaman mempengaruhi operasi bisnis secara signifikan.
High (H)	Ancaman sangat mempengaruhi operasi bisnis.

Setelah semua ancaman yang ada terhadap aset diidentifikasi maka harus dilakukan identifikasi kerentanan di dalam setiap ancaman yang ada. Kerentanan ini akan berkaitan dengan aset- aset dan kontrol yang ada pada setiap aset tersebut, dimana semua kerentanan harus diidentifikasi sesuai dengan ancaman-ancaman yang ada dan sesuai dengan area dimana kerentanan tersebut dapat ditemukan.

Selanjutnya kelemahan akan diberi nilai sesuai dengan kriteria yang ditentukan. Nilai diberikan masih secara kualitatif yang dikemudian akan diberian bobot nilai secara kuantitatif pada tahap analisis risiko. Adapun kriteria yang dipakai dalam melakukan penilaian kelemahan adalah sebagai berikut :

Tabel 3.7 Kriteria Penilaian Kelemahan

Kriteria Penilaian Kelemahan	Deskripsi
Low (L)	Kelemahan aset yang tidak mempengaruhi operasi bisnis walaupun mengakibatkan risiko.

Medium (M)	Kelemahan aset mempe ngaruhi operasi bisnis secara signifikan.
High (H)	Kelemahan aset sangat mempengaruhi operasi bisnis dan harus segera ditangani.

3.4. Perancangan Sistem Keamanan Informasi

Perancangan SMKI yang akan dibangun berupa dokumentasi yang menyediakan tujuan, sasaran dan rencana dari kegiatan untuk mencapai keamanan sumber daya kritikal dalam melindungi informasi yang tersedia di lingkungan perusahaan. Rencana keamanan merupakan hal yang strategis, yang dibangun dengan melakukan manajemen risiko. Alur perencanaan SMKI dapat dilihat ***gambar 3.3***

4. IMPLEMENTASI DAN HASIL

Untuk menentukan risiko apa saja yang terdapat dalam organisasi, terlebih dahulu dilakukan penentuan kritikalitas aset untuk masing-masing layanan yang diselenggarakan oleh perusahaan. Penentuan kritikalitas aset ini dilakukan untuk mengetahui seberapa besar pengaruh aset tersebut terhadap kinerja layanan yang diselenggarakan oleh perusahaan berdasarkan pada 3 (tiga) aspek, yaitu: Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan). Dari daftar aset kritikal yang didapat ini, kemudian dapat didentifikasi risiko apa saja yang mungkin terjadi terhadap aset tersebut.

4.1 Identifikasi Aset

Identifikasi aset dilakukan terhadap aset-aset yang tercakup dalam kebijakan keamanan informasi dengan cara mengamati dan menentukan aset yang terkait dengan layanan akademik. Adapun nilai aset dihitung menggunakan rumus [9] :

Nilai aset = NC + NI + NV/3

Dimana :

NC = Nilai Confidentialti

NI = Nilai Integrity

NV = Nilai Availability

Masing-masing dinyatakan dalam satuan nilai kualitatif berupa low, medium dan high. Untuk lebih jelasnya bisa dilihat pada tabel 4.1 di bawah ini :

Tabel 4.1 Identifikasi Aset

No.	Nama Aset		Lokasi Aset	Pemilik Aset	C	I	A
1	Applikasi	▪ Modul Registrasi Ma hasiswa	Sub bag prog	Administrator	M	H	H
		▪ Modul Administrasi keuangan	Sub bag prog	Administrator	M	H	H
		▪ Modul Internal Akade mik	Sub bag prog	Administrator	M	H	H
		▪ Modul Penerimaan Mahasiswa Baru	Sub bag prog	Administrator	M	H	H
2	Aset Informasi	▪ Database	Sub bag prog	Administrator	L	H	H
		▪ Data perancangan sis tem	Sub bag prog	Administrator	L	H	H
		▪ Sistem operasi	Sub bag prog	Administrator	L	H	H

4.2. Analisis Risiko

Analisis risiko dilakukan berdasarkan hasil dari identifikasi kelemahan, ancaman, besar kemungkinan kejadian, dan tingkat dampak yang ditimbulkan. Identifikasi dilakukan berdasarkan hasil temuan-temuan yang telah terjadi di lapangan maupun hasil analisis kemungkinan ancaman yang terjadi. Dari hasil analisis risiko dapat dilihat mana saja risiko yang diterima, dimitigasi, dihindari atau dialihkan. Risiko-risiko yang dimitigasi kemudian akan digunakan sebagai acuan dalam pemilihan kontrol keamanan. Hasil analisis risiko dapat dilihat pada tabel 4.2.

Tabel 4.2 Hasil Analisis Risiko

No.	Nama Aset	Nilai Aset	Kelemahan	Bobot Ketergantungan	Ancaman	Bobot	Frekuensi	Nilai Dampak	Status Dampak	Bobot BD	Nilai Peristiwa Risiko	Status
1	Modul Registrasi Mahasiswa	8	Pembuangan atau	3	Pencurian media atau dokumen	3	1	72	Negligible	1	8	Risiko diterima
			Pemeliaaan ulang media penyimpanan tanpa penghapusan yang tepat.	3	Pencatan ulang dari media dibaur ulang atau dibuang	3	1	72	Negligible	1	8	Risiko diterima
				3	Pengolahan data ilegal	3	1	72	Negligible	1	8	Risiko diterima
			Kurangnya salinan backup	3	Gangguan sistem	3	1	72	Negligible	1	8	Risiko diterima
2	Modul Administrasi keuangan	8	Pembuangan atau	3	Pencurian media atau dokumen	3	1	72	Negligible	1	8	Risiko diterima
			Pemeliaaan ulang media penyimpanan tanpa penghapusan yang tepat.	3	Pencatan ulang dari media dibaur ulang atau dibuang	3	1	72	Negligible	1	8	Risiko diterima
				3	Pengolahan data ilegal	3	1	72	Negligible	1	8	Risiko diterima
			Kurangnya salinan backup	3	Gangguan sistem	3	1	72	Negligible	1	8	Risiko diterima
3	Modul Internal Akademik	8	Pembuangan atau	3	Pencurian media atau dokumen	3	1	72	Negligible	1	8	Risiko diterima
			Pemeliaaan ulang media penyimpanan tanpa penghapusan yang tepat.	3	Pencatan ulang dari media dibaur ulang atau dibuang	3	1	72	Negligible	1	8	Risiko diterima
				3	Pengolahan data ilegal	3	1	72	Negligible	1	8	Risiko diterima
			Kurangnya salinan backup	3	Gangguan sistem	3	1	72	Negligible	1	8	Risiko diterima
4	Modul Penerimaan Mahasiswa Baru	8	Pembuangan atau Pemeliaaan ulang media penyimpanan tanpa penghapusan yang tepat.	3	Pencurian media atau dokumen	3	1	72	Negligible	1	8	Risiko diterima

Dari hasil analisis risiko dari tabel 4.2 dapat ditarik kesimpulan risiko-risiko yang akan dimitigasi adalah
sebagai berikut :

Tabel 4.3 Proses Aset yang dimitigasi

No	Nama Aset	Kelemahan	Ancaman	Status Dampak
1	PC (Personal Computer)	Kurangnya skema per gantian berkala	Kerusakan perangkat keras	Low
		Kelemahan terhadap vol tase yang bervariasi.	Hilangnya pasokan listrik	Low
			Gangguan perangkat keras	Low
			Kerusakan perangkat keras	Low
2	Jaringan	Sambungan kabel buruk	Kegagalan peralatan Telekomunikasi	Medium
		Lalu lintas jaringan yang sen sitif tidak dilindungi	Penyusupan	Negligible
3	Bandwith Manager	Lalu lintas jaringan yang sen sitif tidak dilindungi	Penyusupan	Negligible
		Arsitektur jaringan yang tidak aman	Penyusupan	Negligible
4	Firewall	Lalu lintas jaringan yang sensitif tidak dilindungi	Penyusupan	Negligible
5	Core Switch	Lalu lintas jaringan yang sensitif tidak dilindungi	Penyusupan	Negligible
6	Distribution Switch	Lalu lintas jaringan yang sensitif tidak dilindungi	Penyusupan	Negligible

4.3 Perlakuan risiko

Risiko yang diidentifikasi pada risk register kemudian tangani dengan baik. Tindakan penanganan ini dideskripsikan sesuai saran dari ahli pada bidang yang bersangkutan. Beberapa saran penanganan risiko ini merupakan tindakan pencegahan agar risiko tidak terjadi. Namun untuk beberapa risiko yang tidak bisa diprediksi dan dicegah, penanganannya berupa tindakan recovery.

Perlakuan risiko yang diambil dapat dilihat pada tabel 4.4.

Tabel 4.4 *Risk Register pelayanan Akademik*

No.	Aset	Deskripsi Risiko	Analisis Kerawanan	Inheren			Kontrol yang ada	Residual			
				Kecenderungan	Dampak	Nilai Risiko Akhir		Kecenderungan	Dampak	Nilai Risiko Akhir	NRD
				Min=1, Maks=5	Min=1 , Maks=5			Min=1 , Maks=5	Min=1 , Maks=5		
1	PC (Personal Computer)	Kerusakan perangkat keras	Kurangnya skema per gantian berkala	2	2	Low	penentuan jadwal ser vis atau jadwal per gantian perangkat keras.	1	2	Low	Low
		Hilangnya pasokan listrik	Kelemahan terhadap voltase yang bervaria si.	2	2	Low	Penggunaan UPS	1	2	Low	Low
		Gangguan perangkat keras		2			Penggunaan UPS	1	2	Low	Low
		Kerusakan perangkat keras		2			Penggunaan UPS	1	2	Low	Low
2	Server	Gangguan perangkat keras	Kelemahan terhadap suhu yang bervariasi.	2	2	Low	penggunaan air con ditioner (AC) khusus nya pada jam kerja	1	2	Low	Low
		Kerusakan perangkat keras	Kurangnya skema per gantian berkala	2	2	Low	penentuan jadwal servis atau jadwal pergantian perangkat keras	1	2	Low	Low
		Gangguan perangkat keras	Kelemahan terhadap voltase yang bervariasi.	2	2	Low	Penggunaan UPS	1	2	Low	Low
		Hilangnya pasokan listrik		2	2	Low	Penggunaan UPS	1	2	Low	Low
		Kerusakan perangkat		2	2	Low	Penggunaan UPS	1	2	Low	Low

4.4 Tahap Penentuan Titik Kontrol

Dari hasil identifikasi risiko kemudian dipilih kontrol dan sasaran kontrol ISO/IEC 27001 yang dapat diterapkan sesuai dengan ruang lingkup yang ditetapkan. Sasaran kontrol dapat ditetapkan sebagai sasaran Keamanan Informasi dalam periode waktu tertentu yang digunakan sebagai indikator untuk mengukur efektivitas penerapan SMKI. SMKI sendiri dibangun berdasarkan pendekatan risiko bisnis. Dalam penentuan titik kontrol terdapat dua bagian utama yaitu:

4.4.1 Identifikasi Proses Bisnis

Dalam hal ini yang akan ditinjau adalah data struktur organisasi dan deskripsi kerja masing-masing bagian atau karyawan pada SIM akademik universitas. Serta dilakukan pemahaman secara menyeluruh mengenai organisasi, baik tujuan maupun arah organisasi.

4.4.2 Analisa Risiko

Bentuk kegagalan fungsi sistem informasi ini dapat beraneka ragam, mulai dari gangguan listrik, serangan hacker, virus, pencurian data, denial of services attack (DOS), bencana alam hingga serangan teroris. Perkembangan ini melahirkan beberapa metodologi untuk mengidentifikasi risiko kemungkinan kerusakan aset-aset pendukung proses bisnis organisasi. Oleh karena itu dibutuhkan prediksi besarnya kerugian yang mungkin terjadi sehingga hasil dari identifikasi tersebut dapat digunakan untuk membangun strategi penanganan risiko serta mengetahui dan menentukan prosedur yang akan dibuat.

4.5 Pembuatan Dokumentasi SMKI

Organisasi menunjuk dan membentuk suatu tim pelaksana yang bertanggung jawab terhadap pembuatan, pengelolaan sampai dengan peningkatan SMKI. Pembuatan dokumentasi SMKI sendiri mengadopsi pembuatan dokumentasi SMM seperti yang ditunjukkan pada Gambar 2.2. yang merupakan isi dari dokumentasi SMKI:

4.5.1 Pembuatan Manual Keamanan Informasi (MKI)

Merupakan langkah awal dalam pembuatan dokumentasi SMKI yang berisi komitmen organisasi terhadap

penerapan Keamanan informasi dan pemenuhan persyaratan standar SMKI yang dipilih. MKI memberikan pandangan kedepan bagi organisasi mengenai kebijakan, tujuan Keamanan informasi, sistem-sistem, prosedur dan metodologinya.

4.5.2 Pembuatan Prosedur Keamanan Informasi (PKI)

PKI berisi uraian urutan pekerjaan/ langkah-langkah kegiatan yang saling terkait satu sama lain. PKI dilengkapi dengan identifikasi terhadap aktivitas-aktivitas yang bersifat kritis, dimana pendokumentasian prosedur akan menunjang pelaksanaan proses secara konsisten. Proses pembuatan PKI tidak memilisi format khusus, melainkan dibuat sesuai dengan kronologis fungsi-fungsi dalam perusahaan yang meliputi:

- Tujuan
- Ruang lingkup
- Standar atau klausul
- Kriteria keberhasilan
- Rincian prosedur (PDCA)
- Rekaman mutu yang biasanya digunakan dalam laporan penilikan, data pengujian, pengesahan laporan, laporan audit dsb.
- Istilah dan definisi
- Catatan perubahan.

4.5.3 Pembuatan Instruksi Kerja (IK)

Instruksi kerja dibuat secara sederhana, praktis dan mudah untuk dipahami, hal ini dikarenakan instruksi kerja ditujukan bagi pengguna yang berada pada posisi pelaksana. Uraian dari instruksi kerja meliputi hal-hal berikut:

- Tahap pelaksanan pekerjaan,
- Alat yang digunakan,
- Standar atau parameter, metode pengukuran, pengujian dan pemeriksaan yang digunakan,
- Sumber daya pendukung lain.

4.5.4 Pembuatan Formulir-formulir

Merupakan dokumen berupa catatan/ rekaman sebagai bukti hasil kerja proses yang ada, contohnya; daftar induk dokumen, rekaman audit internal, rekaman tinjauan manajemen dll.

4.5.5 Pembuatan Referensi

Merupakan dokumen kelengkapan SMKI yang terdiri dari dokumen struktur organisasi, uraian tugas, proses bisnis, kebijakan Keamanan informasi, laporan persiraan risiko, sasaran Keamanan informasi, rencana Keamanan informasi, daftar dokumentasi SMKI, statement of applicability, daftar contoh stempel dan rencana pengelolaan risiko.

4.5.6 Verifikasi SMKI

Pada tahapan ini yang dilakukan adalah dengan melakukan verifikasi terhadap persyaratan kelengkapan dokumen yang merupakan persyaratan dari ISO/IEC 27001:2005 yang terdapat pada klausul 4.3.1. selain itu, verifikasi dilakukan untuk menelusuri keterhubungan Dokumentasi SMKI yang dibangun dengan proses PDCA

5. Kesimpulan

- Perancangan sistem keamanan informasi sesuai dengan tujuh kontrol keamanan yang tersebar dalam empat klausa ISO 27001.
- Identifikasi risiko pada proses bisnis dan aset dilakukan dengan mengidentifikasi risiko yang mungkin muncul pada aset-aset yang berkaitan dengan aplikasi SIM akademik serta kelemahan yang mengancam terjadinya risiko. Identifikasi ini akan diukur dan dinilai dengan kriteria tertentu untuk mengetahui level.
- Pembuatan dokumentasi SMKI mengadopsi tata cara pendokumen -tasian SMM dengan melakukan beberapa penyesuaian terhadap ISO 27001:2005. Struktur atau tahapan pembuatan SMKI

DAFTAR PUSTAKA

1. Andiva. Juni 2008. Hirarki Dokumen ISO 9001:2000 http://bonoes. blogspotcom/2008/06/ hirarki-dokumeniso-9001 2000.html (diakses pada 25 Februari 2013)
2. Atsec Information Security Corporation 2007. ISMS Implementation Guide v 1.1.
3. Bank Indonesia. 2001, “Penerapan Manajemen Risiko Bagi Bank Umum” Peraturan Bank Indonesia Nomor 5/8/PBI/2003 Tanggal 19 Mei 2003, Jakarta.
4. Constatin Tofan, Dan. (2011). *Information Security Standars*. Rumania: Academy of Economic Studies Bucharest.
5. Diskominfo, (2011). Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik.
6. Howard, John. (1997). An Analysis of Security Incident on The Internet 1989-1995. Pittsburgh : Carneige Mellon University.
7. ISO/IEC 27001 : 2005. *Information technology — Security techniques- Information security management systems — Requirements.*
8. ISO/IEC 27005 : 2008. *Information technology - Security techniques- Information security risk management.*
9. Johnson, Brad C. 2008. Information Security Basics.
10. Kamat, Mohan. 2009. *Guideline for Information Asset Valuation*.
11. Kamat, Mohan. 2009. *Guideline for Non Information (Physical) Asset Valuation*.
12. Kamat, Mohan. 2009. *Guideline for People Asset Valuation*.
13. Kamat, Mohan. 2009. *Matrices for Asset Valuation and Risk Analysis*.
14. Peltier, T. R. (2001). *Information Security Risk Analysis. Aurbach Publications.*
15. R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson. (2007). *Introduction OCTAVE Allegro : Improving the Information Security Risk Assesment Process.*
16. Rothery, Brian. 1996. Anaiisis ISO 9000, PT. Pustaka Binaan Pressindo.

17 Salazar, Vima. 2006. Management of Information Security Good Practice Note.
18. SANS Institute, (2004). Designing And Implmenting An Effective *Information Security Program : Ptotecting the Data Assets of Individuals, Small And Large Businesses*.
19. Sarno, Riyanarto., Iffano, Irsyat. (2009). Sistem Manajemen Keamanan Informasi. ITSPress.
20. Setiawan, Bambang. 2008. Pengantar Keamanan Komputer.
21. Turban, Effrain, Rainer R. Kelly Jr., & Potter Richard E. (2006). *Introduction To Information Technology*, Edisi ke-3. Terjemahan Kwary, Deny Armos & Sari, Dewi Fitria. Salemba Infortek, Jakarta.