PERENCANAAN DAN IMPLEMENTASI SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2005 (Studi Kasus Pada Sebuah Bank Swasta Nasional)

Nugroho Arif Widodo[*)], R. Rizal Isnanto, and Adian Fatchur Rochim

Jurusan Teknik Elektro, Universitas Diponegoro Semarang
Jl. Prof. Sudarto, SH. Kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)]*E-mail : nawidodo@gmail.com*

Abstrak

Informasi merupakan suatu elemen yang sangat penting bagi organisasi masa kini. Kerahasiaan, integritas, dan ketersediaan informasi memiliki peran yang vital dalam menunjang kinerja organisasi. Oleh karena itu, mutlak diperlukan suatu tindakan pengamanan informasi agar penggunaan informasi dapat berjalan secara efektif, efisien, dan terpadu.Sebuah sistem manajemen keamanan informasi (SMKI) adalah seperangkat kebijakan yang berkaitan dengan manajemen keamanan informasi. Prinsip yang mengatur di balik SMKI adalah bahwa organisasi harus merancang, menerapkan dan memelihara seperangkat kebijakan, proses dan sistem untuk mengelola risiko aset informasi mereka, sehingga memastikan tingkat risiko keamanan informasi yang dapat diterima.Penelitian ini bertujuan untuk membantu merancang, mengimplementasikan, mengoperasikan, memonitor, memelihara, dan meningkatkan pengamanan informasi pada sebuah bank swasta nasional.Dari perencanaan dan implementasi sistem manajemen keamanan informasi ini, dihasilkan daftar nilai risiko akhir aset-aset kritikal dan dokumen-dokumen tata kelola penunjang SMKI. Penelitian ini juga menghasilkan beberapa rekomendasi untuk perbaikan proses pengamanan informasi yang dapat digunakan untuk meningkatkan keamanan informasi serta menjadi acuan untuk memperoleh sertfikasi sistem manajemen keamanan informasi dengan standar ISO/IEC 27001:200.

Kata-kunci: keamanan, informasi, risiko, ISO/IEC 27001:2005

Abstract

Information is a very important element for today's organizations. Confidentiality, integrity, and availability of information has a vital role in supporting organizational performance. Therefore, it is absolutely necessary an information security measure in order to use the information to run effectively, efficiently, and integrated. An information security management system (ISMS) is a set of policies related to information security management. Governing principle behind ISMS is that an organization should design, implement and maintain a set of policies, processes and systems to manage the risk of their information assets, thereby ensuring information security risk level is acceptable. This study aims to help design, implement, operate, monitor, maintain, and improve the security of information on a national private banks. Of planning and implementation of the information security management system, resulting lists final risk value assets and critical documents supporting ISMS governance. The study also produced several recommendations for improvement of information security process that can be used to improve the security of information as well as a reference to obtain certification of information security management system standard ISO / IEC 27001:2005.

Keyword :security, information, risk, ISO / IEC 27001:2005

1. Pendahuluan

Informasi adalah aset yang sangat penting bagi sebuah Bank, baik informasi yang terkait dengan nasabah, keuangan, laporan maupun informasi lainnya. Kebocoran, kerusakan, ketidak akuratan, ketidak tersediaan atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik secara finansial maupun non-finansial bagi Bank. Dampak dimaksud tidak hanya terbatas pada Bank tersebut, namun juga nasabah, Bank lain dan bahkan terhadap sistem perbankan nasional. Mengingat pentingnya informasi, maka informasi harus dilindungi atau diamankan oleh seluruh personil di Bank. Pengamanan informasi sangat bergantung pada pengamanan terhadap semua aspek dan komponen TI

terkait, seperti perangkat lunak, perangkat keras, jaringan, peralatan pendukung (misalnya sumber daya listrik dan AC) dan sumber daya manusia (termasuk kualifikasi dan ketrampilan). Salah satu kebijakan yang dapat diambil oleh perusahaan untuk mengatasi gangguan keamanan informasi adalah dengan menerapkan Sistem Manajemen Keamanan Informasi (SMKI)[5].

Penerapan Sistem Manajemen Keamanan Informasi saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik mengingat peran Teknologi Informasi dan Komunikasi (TIK) yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik. Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan, keutuhan dan ketersediaan[17].Mengingat pentingnya informasi, maka kebijakan tentang pengamanan informasi harus mencakup sekurang-kurangnya terdapat prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik dan lingkungan, prosedur pengamanan logical security, prosedur pengamananoperasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi[5]. Untuk itu diperlukan perencanaan danimplementasi sistem manajemen keamanan informasi untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur. Standar yang digunakan yaitu ISO/IEC 27001:2005. Beberapa hal penting yang patut dijadikan pertimbangan mengapa standar ISO/IEC 27001:2005 dipilih karena dengan standar ini sangat fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dan ukuran struktur organisasi serta ISO/IEC 27001:2005 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara internasional[3].Penelitian penelitian ini bertujuan untuk merancang sebuah Sistem Manajemen Keamanan Informasi (SMKI) yang mengacu pada standar internasional ISO/IEC 27001:2005.

2. Metode

2.1 Keamanan Informasi

Keamanan informasi berkaitan dengan perlindungan aset berharga terhadap kehilangan, pengungkapan penyalahgunaan, 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 tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis[14].

Organisasi keamanan informasi memiliki tiga aspek yang harus dipahami untuk bisa menerapkannya, aspek tersebut biasa disebut dengan CIA Triad Model, yang antara lain adalah[10]:

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). Merupakan aspek yang memberi jaminan atas ketersediaan data saat dibutuhkan, kapanpun dan dimanapun.

Selain aspek di atas, keamanan informasi dapat juga diklasifikasikan sebagai berikut[15]:

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

2.2 Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi (SMKI) adalah cara untuk melindungi dan mengelola informasi berdasarkan pendekatan risiko bisnis yang sistematis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara, dan meningkatkan keamanan informasi[2]. SMKI adalah sebuah pendekatan organisasi untuk keamanan informasi. Sebagai sebuah sistem, SMKI harus didukung oleh keberadaan dari hal-hal berikut:

1. Struktur organisasi, biasanya berupa keberadaan fungsi-fungsi atau jabatan organisasi yang terkait dengan keamanan informasi, misalnya *Chief Information Security Officer* (CISO).
2. Kebijakan keamanan, berupa peraturan yang mengatur pelaporan semua kejadian pelanggaran keamanan, kelemahan sistem informasi, serta pengambilang langkah-langkah penanggulangan yang perlu.
3. Prosedur dan proses, yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan. Misalnya prosedur pengelolalan fasilitas internet.
4. Tanggung jawab, yang dimaksud dengan tanggung jawab adalah tercerminnya konsep dan aspek-aspek keamanan informasi perusahaan di dalam deskripsi tugas setiap jabatan dalam perusahaan. Begitu pula dengan adanya program-program pelatihan serta pembinaan tanggung jawab keamanan informasi perusahaan untuk staf dan karyawannya.
5. Sumber daya manusia, adalah pelaksana serta objek pengembangan keamanan informasi di perusahaan.

Tahap pendokumentasian SMKI mengadopsi pada pendokumentasian Sistem Manajemen Mutu (SMM). Setiap aktivitas dan proses yang dilakukan pada SMKI merupakan representasi dari siklus hidup PDCA. Salah satu proses yang penting dari SMKI adalah proses identifikasi resiko yang bertujuan untuk mengetahui prosedur-prosedur apa saja yang perlu dibuat untuk mengamankan dan melindungi aset informasi organisasi.

2.3 Sistem Manajemen Mutu

Mutu adalah perpaduan sifat-sifat dan karakteristik yang menentukan sampai seberapa jauh keluaran yang dihasilkan suatu perusahaaan atau organisasi dapat memenuhi kebutuhan pembelinya[13]. Tujuan mutu sendiri adalah memberikan keyakinan bahwa produk atau jasa yang dihasilkan perusahaan memenuhi persyaratan mutu pembeli. Sistem mutu mencakup jaminan mutu dan pengendalian mutu. Jaminan mutu adalah istilah untuk menyatakan keseluruhan kegiatan yang terencana dan resmi dalam rangka memberi kepercayaan bahwa output yang dimaksud akan memenuhi tingkat mutu yang diinginkan[6]. Sistem mutu sendiri adalah program perencanaan kegiatan sumber daya yang didorong oleh manajemen dan berlaku di seluruh organisasi.

ISO 9001 merupakan standar utama bagi perusahaan yang ingin memberikan jaminan mutu kepada pelanggannya. Standar yang dimaksudkan mencakup keseluruhan tahapn proses mulai dari desain, pengembangan produksi, instalasi sampai dengan jasa.. Pembuatan dokumentasi SMM sendiri dipandang sebagai kegiatan yang memberikan nilai tambah dan bukan menjadi tujuan akhir dari pembuatan SMM.

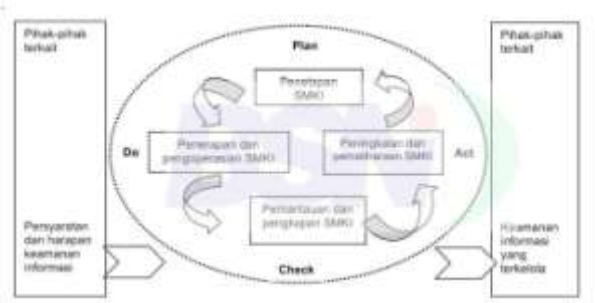
Gambar 1 Piramida dokumentasi SMM[1]

Dari Gambar 1 dapat dijelaskan masing-masing tahapan pada proses dokumentasi SMM:

1. Pedoman/manual merupakan kunci utama dalam dokumentasi sistem. Panduan mutu menerangkan dengan jelas kepada setiap orang mengenai komitmen perusahaan terhadap mutu dengan cara memberikan pandangan kedepan, kebijakan, tujuan, sistem, prosedur dan metodologi.
2. Prosedur mutu, adalah prosedur yang menjelaskan langkah serta mekanisme pelaksanaan semua proses aktifitas dalam sistem penjaminan mutu yang melibatkan berbagai fungsi[12].
3. Instruksi kerja, tidak terdapat format khusus dalam pembuatannya, hanya berupa urutan langkah demi langkah. Instruksi kerja dapat berupa narasi, diagram alir, gambar dll.
4. Form/record, merupakan dokumen berupa catatan mutu, sebagai bukti hasil kerja masing-masing proses yang ada, contohnya: daftar induk dokumen, rekaman audit internal, rekaman tinjauan manajemen dll[1].

2.4 Model Plan-Do-Check-Act (PDCA)

PDCA adalah suatu proses pemecahan masalah yang digunakan dalam pengendalian mutu. Metode ini dipopulerkan oleh W. Edwards Deming yang dianggap sebagai bapak pengendalian mutu modern, sehingga sering disebut dengan siklus Deming[11]. Masukan dalam model ini berupa kebutuhan keamanan informasi dan ekspektasi, sedangkan keluaran yang dihsailkan berupa pengaturan keamanan informasi. Demikian pada Gambar 2 ditunjukkan siklus PDCA.



Gambar 2 Model PDCA[7]

Penjelasan dari siklus PDCA adalah sebagai berikut:

1. Plan (penetapan SMKI)

Tahap Plan adalah tahap penetapan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan keluaran yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.

2. Do (penerapan dan pengoperasian SMKI)

Tahap Do adalah tahap dimana solusi dan perubahan dari proses yang telah direncanakan dilaksanakan. Pelaksanaan yang dilakukan adalah penerapan prosedur-prosedur serta instruksi kerja sesuai dengan aktivitas yang terjadi dalam organisasi.

3. Check (pemantauan dan pengkajian SMKI)

Tahap Check merupakan tahapan untuk menilai dan mengukur proses pengamanan informasi terhadap kebijakan, prosedur, dan best practices serta melaporkan hasilnya pada tinjauan manajemen

4. Act (peningkatan dan pemeliharaan SMKI)

Tahap Act merupakan tahapan untuk melakukan tindakan pencegahan dan perbaikan berdasarkan hasil Audit Internal SMKI, tinjauan manajemen dan informasi terkait untuk menghasilkan peningkatan SMKI yang berkesinambungan.

2.5 ISO/IEC 27001:2005

ISO/IEC 27001:2005 merupakan standar keamanan informasi yang menggantikan BS-7799:2 dan diterbitakan pada bulan Oktober 2005 oleh International Organization for Standarization dan International Electrotechnical Commission[4]. Tujuan pembuatan standar ini adalah untuk menciptakan sebuah panduan pembuatan, penerapan, pelaksanaan, pengawasan, analisis, pemeliharaan, dan pendokumentasian Sistem Manajemen Keamanan Informasi (SMKI) yang dapat diacu oleh berabagai jenis organisasi, seperti perusahaan swasta, lembaga pemerintahan, dan organisasi nirlaba. ISO/IEC 27001:2005 didesain untuk memastikan bahwa kendali keamanan yang dibuat untuk melindungi aset-aset informasi dan menciptakan kepercayaan dengan pihak-pihak yang terkait sudah memadai dan sesuai[9].

2.6 Pengumpulan Data

Pengumpulan data dilakukan untuk mendapatkan pemahaman mengenai proses bisnis yang berjalan serta permasalahan yang dihadapi perusahaan. Pengumpulan data dilakukan dengan dua cara yaitu observasi langsung serta wawancara terhadap personil organisasi.

2.6.1 Observasi

Observasi dilakukan dengan pengamatan secara langsung pada perusahaan sehingga diketahui kondisi nyata dari perusahaan tersebut. Observasi ini dilakukan pada InfoSec Division di beberapa seksi antara lain:
1. IS Operation Section
2. IS Policy & Standard Section
3. IT Compliance & Risk Management Section
4. ID Management Section

Melalui tahapan observasi yang telah dilakukan, diperoleh informasi mengenai aset-aset pendukung operasional yang digunakan sebagai pengolah informasi.

2.6.2 Wawancara

Wawancara dilakukan terhadap personil terkait dengan pelaksanaan tugasnya sehari-hari yang berhubungan langsung dengan permasalahan pengolahan dan keamanan informasi. Melalui tahapan wawancara diperoleh informasi mengenai tugas pokok dan fungsi masing-masing bagian, penggunaan dan permasalahan aset pendukung operasional terutama perangkat pengolah informasi hasil observasi, serta permasalahan dan ancaman/risiko yang berkaitan dengan keamanan informasi.

3. Hasil dan Analisis

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.Aset-aset kritikal yang sudah teridentifikasi tersebut kemudian dimasukkan ke dalam Tabel 1 dibawah ini.

Tabel 1 Contoh daftar Aset Kritikal

No	Aset	Uraian
Aset Sumber Daya Manusia		
1	Pegawai tetap	
Aset Fisik		
2	PC	
Aset Perangkat Lunak		
3	Sistem operasi	
Aset Jaringan Komunikasi dan Data		
4	Hub/Switch	
Aset Sarana Pendukung		
5	Listrik	

Selanjutnya adalah mengidentifikasi ancaman dan kerawanan yang mengancam keberadaan informasi sebagai aset berharga perusahaan. Ancaman terhadap aset karena adanya kelemahan sistem itu sendiri yang harus diwaspadai karena akan berdampak pada proses bisnis yang ada. Terutama jika dampak yang ditimbulkan akibat bencana alam memerlukan waktu, tenaga dan biaya yang untuk pemulihan yang cukup besar.

3.1 Evaluasi Risiko

Tahap evaluasi risiko merupakan tahap untuk melakukan penyusunan dan pengorganisasian risiko yang diperoleh dari kegiatan identifikasi risiko, dengan melakukan penilaian risiko dan membuat strategi mitigasi sebagai mekanisme perlindungan keamanan informasi yang efektif dan efisien disertai tindakan perbaikan yang dapat diimplementasikan institusi.
Aktivitas yang dilakukan dalam evaluasi risiko dimulai dengan menilai probabilitas atau kecendrungan terjadinya ancaman dalam sekala periode tertentu disertai frekuensi kejadian serangan seperti yang ditunjukkan pada Tabel 2.

Tabel 2 Penilaian kecenderungan risiko

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

Kemudian penilaian terhadap dampak yang dihasilkan bagi perusahaan akan ditunjukkan Tabel 3 berikut ini. Dampak diklasifikasikan berdasarkan beberapa parameter seperti operasional, kinerja, reputasi dan finansial.

Tabel 3 Penilaian dampak risiko

Tingkat Dampak	Operasional	Kinerja	Reputasi	Finansial
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
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
3	Menimbulkan penundaan aktivitas (proses tidak Dapat dijalankan) Maksimum selama 2 hari	Menimbulkan gangguan kegiatan pada kegiatan operasional layanan pendukung	Terdapat citra negatif yang dapat mempengaruhi kinerja atau kebijakan	Kerugian atau biaya yang harus dikeluarkan Rp 10.000.001 hingga Rp 50.000.000
2	Menimbulkan penundaan aktivitas (proses tidak dapat dijalankan) maksimum selama 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 Rp 1.000.001
1	Tidak menimbulkan penundaan aktivitas	Tidak terjadi gangguan pada proses layanan	Tidak ada publikasi	Kerugian atau biaya yang harus dikeluarkan dibawah Rp 1.000.000

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 4 berikut ini akan disajikan matriks penilaian dari nilai risiko dasar.

Tabel 4 Matriks analisis risiko dasar

		Tingkat Dampak				
		1	2	3	4	5
Tingkat Kecenderungan	1	Rendah				
	2					
	3		Sedang			
	4				Tinggi	
	5					

Berdasarkan hasil penilaian risiko yang didapatkan dari proses identifikasi dan analisis risiko pada Tabel 4 selanjutnya dilakukan beberapa tindakan yang diperlukan seperti ditunjukkan pada Tabel 5 berikut. Apabila nilai risiko “Sedang” atau “Tinggi” maka jenis pengendalian adalah “Kontrol” atau dibutuhkan kontrol tambahan untuk meminimalisir risiko.

Tabel 5 Nilai Pengendalian

Nilai/ Warna	Kriteria Pengendalian	Keterangan
1	Lemah	Pelaksanaan kontrol tidak berjalan baik dan tidak dimonitor sehingga tidak mempengaruhi tingkat risiko.
2	Sedang	Pelaksanaan kontrol tidak berjalan konsisten dan terjadi berulang kembali sehingga tidak sepenuhnya mampu mengurangi atau meminimalkan tingkat risiko
3	Kuat	Penerapan kontrol sudah cukup baik dan konsisten sehingga dapat mengurangi/meminimalkan tingkat risiko.

Selanjutnya untuk mencari nilai risiko akhir digunakan matriks dengan parameter dari nilai risiko dasar dan nilai pengendalian seperti pada Tabel 6 berikut ini:

Tabel 6 Matrik nilai risiko akhir

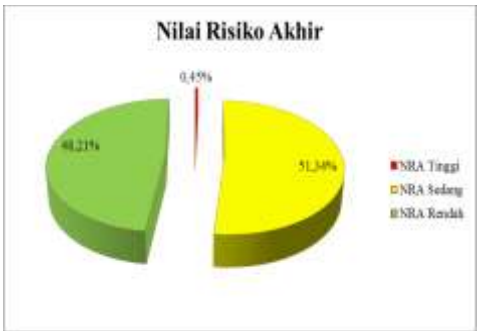
		Nilai Risiko Dasar		
		Rendah	Sedang	Tinggi
Nilai Pengendalian	Lemah	Sedang	Sedang	Tinggi
	Sedang	Rendah	Sedang	Tinggi
	Kuat	Rendah	Rendah	Sedang

3.2 Komposisi Risiko

Secara umum gambaran kondisi risiko di dalam organisasi dapat dilihat dari nilai risiko akhir dan persebaran risiko yang didapat dari proses *Risk Assessment* yang dilakukan. Berdasarkan nilai risiko akhirnya dapat digambarkan dalam Tabel 7 dan Gambar 3.

Tabel 7 Komposisi Nilai Risiko Akhir

Jenis NRA	Section	Jumlah NRA	Total
Rendah	IS Operation Section	31	108
	IS Policy & Standard Section	25	
	IT Compliance & Risk Management Section	23	
	ID Management Section	29	
Sedang	IS Operation Section	36	115
	IS Policy & Standard Section	17	
	IT Compliance & Risk Management Section	37	
	ID Management Section	25	
Tinggi	ID Management Section	1	1



Gambar 3 Komposisi Nilai Risiko Akhir

Nilai risiko akhir bersifat tinggi berjumlah 0,45%, NRA sedang 51,34%, dan NRA rendah berjumlah 48,21%. Oleh karena itu, sangat perlu diberikan penanganan karena risiko-risiko ini memiliki dampak yang tinggi jika sampai terjadi. Komposisi 51,34% nilai risiko bersifat sedang menunjukkan masih terdapat banyak kerawanan yang meskipun telah diberikan kontrol namun masih dapat dieksploitasi untuk menyebabkan terjadinya risiko. Dengan demikian risiko-risiko yang bernilai akhir sedang ini perlu untuk diberi kontrol tambahan untuk lebih memperkecil kemungkinan dan dampak terjadinya risiko tersebut. Rendahnya nilai risiko akhir ini didapat karena sifat dasar risiko yang memang rendah atau karena organisasi telah menerapkan kontrol-kontrol yang sesuai untuk menurunkan nilai akhir risiko-risiko tersebut.

Pola lain yang ditunjukkan dari hasil *Risk Assessment* adalah pola persebaran risiko, yang dapat digambarkan dalam Tabel 8 dan Gambar 4.

Tabel 8 Persebaran Nilai Risiko Akhir

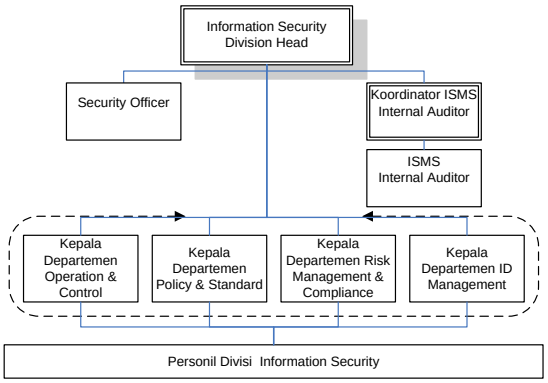
	IS Operation Section	IS Policy & Standard Section	IT Compliance & Risk Management Section	ID Management Section
Rendah	31	25	23	29
Sedang	36	17	37	25
Tinggi	0	0	0	1

Gambar 4 Persebaran Nilai Risiko Akhir

Dalam diagram tersebut dapat dilihat bahwa sebagian besar risiko diidentifikasi terdapat pada bagian-bagian dalam InfoSec Division yang disediakan oleh bagian IS Operation (sebanyak 29,91%). Pada tabel juga dapat kita lihat bahwa

ID Management merupakan satu-satunya departemen yang memiliki risiko dengan nilai risiko akhir bersifat "tinggi" sejumlah 1 risiko, sedangkan IS Policy & Standard memiliki resiko paling sedikit (sebanyak 18,75%).

Sebelum melakukan pembuatan dokumen tata kelola SMKI, organisasi harus menunjuk dan membentuk tim pelaksana pembuatan tata kelola SMKI. Hal tersebut penting dilakukan karena tata kelola SMKI merupakan suatu sistem keamanan yang penerapannya adalah tanggung jawab semua pihak, mulai dari *top level management* (manajemen tingkat atas) sampai ke level yang paling bawah. Struktur organisasi tim pelaksana tata kelola SMKI dapat dilihat pada Gambar 5



Gambar 5 Struktur organisasi SMKI

Pembuatan dokumen didasarkan pada klausul yang terdapat pada ISO/IEC 27001:2005, dan mengadopsi piramida pembuatan dokumentasi standar manajemen mutu. Dokumen tata kelola keamanan informasi dapat digambarkan secara garis besar seperti dibawah ini:

1. Manual Keamanan Informasi(MKI)

Tahap ini merupakan langkah awal dalam pembuatan dokumentasi tata kelola SMKI yang berisi komitmen perusahaan dalam menerapkan keamanan informasi dan pemenuhan persyaratan standar SMKI yang dipilih. MKI memberikan pandangan kedepan bagi perusahaan mengenai kebijakan, tujuan keamanan informasi, sistem-sistem dan metodologinya. Struktur penulisan dokumen MKI antara lain:

2. Prosedur Keamanan Informasi

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 memiliki format khusus, melainkan dibuat sesuai dengan kronologis fungsi-fungsi dalam perusahaan

3. Instruksi Kerja

Instruksi kerja dibuat secara sederhana, praktis dan mudah untuk dipahami, hal ini dikarekanan instruksi kerja ditujukan bagi pengguna yang berada pada posisi pelaksana

4. Formulir

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

5. Referensi

Merupakan dokumen kelengkapan SMKI yang terdiri dari dokumen struktur organisasi, uraian tugas, proses bisnis, kebijakan informasi, laporan perkiraan risiko, sasaran kemanan informasi, rencana keamanan informasi, daftar dokumetasi SMKI, *statement of applicability* (pernyataan pemberlakuan), dan rencana pengelolaan risiko.

4. Kesimpulan

Simpulan yang dapat diambil dari penelitian ini antara lain setelah dilakukan penelitian terhadap aspek-aspek manajemen keamanan informasi maka telah dapat disusun sebagai Sistem Manajemen Keamanan Informasi (SMKI) yang mengacu pada standar Internasional ISO/IEC 27001:2005 pada organisasi.Berdasarkan hasil penelitian yang dilakukan dapat diketahui bahwa komposisi Nilai Risiko Akhir (NRA) pada organisasi adalah NRA tinggi berjumlah 0,45%, NRA sedang 51,34 %, dan NRA rendah berjumlah 48,21%. Hal ini menunjukkan bahwa nilai risiko akhir cenderung berkategori sedang. Terlihat bahwa sebagian besar risiko diidentifikasi terdapat pada bagian-bagian dalam InfoSec Division yang disediakan oleh bagian IS Operation (sebanyak 29,91%). Pada penelitian ini juga dapat kita lihat bahwa ID Management merupakan satu-satunya departemen yang memiliki risiko dengan nilai risiko akhir bersifat "tinggi" sejumlah 1 risiko, sedangkan IS Policy & Standard memiliki resiko paling sedikit (sebanyak 18,75%).Manfaat dari penelitian ini adalah dokumen tata kelola yang dihasilkan diharapkan dapat membantu pengelolaan keamanan informasi sehingga akan meningkatkan kinerja dari perusahaan. Saran untuk penelitian selanjutnyadilakukan dalam semua fase Plan-Do-Check-Act (PDCA), menggunakan framework selain ISO/IEC 27001:2005, misal COBIT atau ITIL, untuk dibandingkan dengan metode yang dipakai pada penelitian ini, kemudian disimpulkan metode mana yang terbaik.

Referensi

[1]. Andiva. Juni 2008. Hirarki Dokumen ISO 9001:2000 http://bonoes.blogspotcom/2008/06/hirarki-dokumen-iso-9001-2000.html (diakses pada 25 Februari 2013)

[2]. Atsec Information Security Corporation 2007. ISMS Implementation Guide v 1.1.

[3]. British Standards Institution. 2008. ISO/IEC 27001 Features and Benefits.

[4]. Calder, Alan., Steve Watkins. 2008. IT Governance - A Managers Guide to Data Security and ISO 27001 - ISO 27002
[5]. Direktorat Penelitian dan Pengaturan Perbankan. 2007. Pedoman Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum.
[6]. Hadiwiardjo, H. B. Wibisono, dkk. Juli 1996. ISO 9000 Sistem Manajemen Mutu. Ghalia Indonesia.
[7]. INB. November 2005. Information-technology-security techniques-information security management system-requirements.
[8]. Ismiatin, Rahayu. 2009. Analisis Risiko Proyek Perusahaan
[9]. ISO/IEC 27001:2005, Information Technology – Security Techniques -- Information security management systems – Requirements
[10]. Johnson, Brad C. 2008. Information Security Basics.
[11]. Moen, Roland. 2009. Evolution of the PDCA Cycle.
[12]. Pranashakti, Ipan. Maret 2009. Pengertian prosedur mutu. http://ipan.staffuii.ac.id/2009/02/perangkat-sistem-penjaminan-mutu-uii-Yogyakarta. (diakses pada 25 Februari 2013)
[13]. Rothery, Brian. 1996. Anaiisis ISO 9000, PT. Pustaka Binaan Pressindo.
[14]. Salazar, Vima. 2006. Management of Information Security Good Practice Note.
[15]. Setiawan, Bambang. 2008. Pengantar Keamanan Komputer.
[16]. Syafrizal, Melvin. 2008. Information Security Management System (ISMS) Menggunakan ISO/IEC 27001:2005.
[17]. Tim Direktorat Keamanan Informasi Depkominfo. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik.