BAB II

LANDASAN TEORI

2.1 Audit

Penggunaan istilah audit telah banyak dipakai di berbagai disiplin ilmu, mulai dari keuangan, pemerintahan hingga Teknologi Informasi (TI). Audit merupakan proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan (Sarno, 2009).

Dalam melaksanakan audit terdapat dua jenis audit yaitu: audit kepatutan dan audit subtansi. Pelaksanaanya tergantung dengan kebutuhan dan tujuan audit itu sendiri (dapat dilakukan secara terpisah). Beberapa jenis audit yaitu:

a. Audit Kepatutan (*Compliance Audit*)

Audit kesesuaian adalah audit Sistem Manajemen Keamanan Informasi (SMKI) yang dilaksanakan untuk tujuan menegaskan apakah Objektif Kontrol, Control dan prosedur memenuhi hal berikut:

- Telah memenuhi persyaratan sebagaimana ditulis dalam manual Sistem Manajemen Keamanan Informasi (SMKI).
- Telah efektif diterapkan dan digunakan.
- Telah berjalan dengan yang diharapkan.

b. Audit Subtansi (*Subtantion Audit*)

Dalam audit keamanan informasi pada bagian pengembangan multimedia baru ini menggunakan audit subtansi yaitu subuah langkah audit SMKI yang

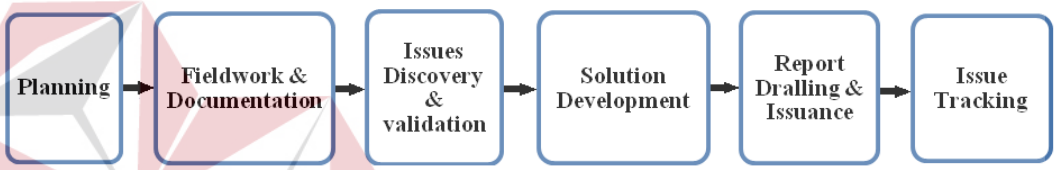
dilaksanakan untuk tujuan menegaskan apakah hasil dari aktifitas (prosedur atau proses telah dijalankan) telah sesuai dengan yang ditargetkan atau yang diharapkan.

Selanjutnya aktivitas yang berlangsung pada dasarnya serupa, yakni: penemuan ketidakpatutan proses yang ada terhadap standar pengelolaan aktivitas terkait. Agar dapat sukses mengimplementasikan hal tersebut, maka aktivitas audit seharusnya terencana dengan baik untuk memberikan hasil yang optimal sesuai dengan kondisi bisnis masing-masing perusahaan (Sarno, 2009). Beberapa tinjauan penting elemen utama dalam Audit dapat diklasifikasikan sebagai berikut:

1. Tinjauan terkait fisik dan lingkungan, yakni: proses yang terkait dengan faktor lingkungan, keamanan fisik, suhu udara, kontrol kelembaban, dan suplai sumber daya.
2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem manajemen basis data, sistem operasi, pelaksana, dan seluruh prosedur administrasi sistem.
3. Tinjauan perangkat lunak. Perangkat lunak yang dimaksud adalah proses informasi. Mencakup kontrol akses dan otorisasi ke dalam sistem, validasi dan penanganan kesalahan termasuk pengecualian dalam sistem serta aliran proses informasi dalam perangkat lunak beserta kontrol secara manual dan prosedur penggunaannya. Sebagai tambahan, tinjauan juga perlu dilakukan terhadap siklus hidup pengembangan sistem.
4. Tinjauan kemanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung ke dalam sistem, batasan tingkat keamanan,

tinjauan terhadap *firewall*, daftar kontrol akses *router*, *port scanning* serta pendeteksian akan gangguan maupun ancaman terhadap sistem.

5. Tinjauan kontinuitas bisnis dengan memastikan ketersediaan prosedur penyimpanan dan duplikasi informasi, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana atau kontinuitas bisnis yang dimiliki.
6. Tinjauan integritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kontrol keamanan dan dampak dari kurangnya kontrol yang diterapkan.



Gambar 2.1 Gambaran Proses Audit
(Sumber: Davis, 2011)

Menurut (Davis, 2011) beberapa tahapan audit seperti yang terlihat pada Gambar 2.1, setiap tahapan-tahapan akan dijelaskan sebagai berikut:

1. *Planning*

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

2. *Fieldwork and Documentation*

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

3. *Issues Discovery and Validation*

Pada tahap ini auditor harus menentukan dan melakukan perbaikan pada daftar isu-isu yang potensial untuk memastikan isu-isu yang valid pada relevan. Auditor harus mendiskusikan isu-isu potensial dengan pelanggan secepat mungkin. Selain memvalidasi bahwa fakta-fakta telah benar, maka perlu memvalidasi bahwa resiko yang disajikan oleh masalah ini cukup signifikan memiliki nilai untuk pelaporan dan pengalamatan.

4. *Solution Development*

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

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

5. *Report Drafting and Issuance*

Setelah ditemukan masalah dalam lingkungan yang diaudit, memvalidasi, dan mendapatkan solusi yang dikembangkan untuk mengatasi masalah, maka langkah selanjutnya adalah membuat draft untuk laporan audit. Laporan audit adalah sebagai dokumen hasil audit. Fungsi utama laporan audit:

a. Untuk auditor dan instansi yang diaudit, berfungsi sebagai catatan audit, hasilnya, dan rencana rekomendasi yang dihasilkan
b. Untuk Kepala Seksi dan auditor, berfungsi sebagai "kartu laporan" pada bagian yang telah diaudit.

6. *Issue Tracking*

Audit belum benar-benar lengkap sampai isu yang diangkat dalam audit tersebut diselesaikan. Bagian PMB harus mengembangkan suatu proses dimana karyawan dapat melacak dan mengikuti sampai isu terselesaikan. Auditor yang melakukan atau memimpin audit bertanggung jawab untuk menindak lanjuti poin dari audit seperti tanggal jatuh tempo untuk setiap pendekatan dari audit yang dihasilkan.

Penentuan metode dan tahapan penelitian audit keamanan informasi pada bagian PMB dilakukan dengan mengacu dari proses audit oleh (Davis, 2011) serta dikembangkan menjadi metode yang lebih kompatibel untuk memperoleh data yang akurat dan relevan. Setiap tahapan dan metode penelitian audit sistem informasi akan digambarkan dalam Tabel 2.1:

Tabel 2.1 Tahapan dan metode penelitian audit keamanan informasi

No.	Tahapan Davis	Metode
1.	- Plainning	- Perencanaan audit - Persiapan audit
2.	- Fieldwork and documentation - Issues discovery and validation - Solution development	- Pelaksanaan audit
3.	- Report drafting and issuance	- Pelaporan audit

2.2 Sistem Informasi

Sistem adalah suatu *entity* yang terdiri dari dua atau lebih komponen yang saling berinteraksi untuk mencapai tujuan (Mukhtar, 1999). Sistem adalah sekelompok dua atau lebih komponen-komponen yang saling berkaitan (*inter-related*) atau subsistem-subsistem yang bersatu untuk mencapai tujuan yang sama (*common purpose*) (Gondodiyoto, 2007).

Informasi berarti hasil suatu proses yang terorganisasi, memiliki arti dan berguna bagi orang yang menerimanya (Mochtar, 1999). Informasi menyebabkan pemakai melakukan suatu tindakan yang dapat dilakukan atau tidak dilakukan (Hall, 2001). Informasi ditentukan oleh efeknya pada pemakai, bukan oleh bentuk fisiknya (Gondodiyoto, 2007).

Dengan demikian sistem informasi dapat didefinisikan sebagai kumpulan elemen/sumberdaya dan jaringan prosedur yang saling berkaitan secara terpadu, terintegrasi dalam suatu hubungan hirarkis tertentu dan bertujuan untuk mengolah data menjadi informasi (Gondodiyoto, 2007).

2.3 Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimalisi risiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Sarno dan Iffano, 2009). Contoh Keamanan Informasi menurut (Sarno dan Iffano, 2009) adalah:

1. *Physical Security* adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik dan tempat kerja dari berbagai ancaman meliputi akses tanpa otoritasi, kebakaran, dan bencana alam.
2. *Personal Security* adalah Keamanan Informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup (*physical security*).
3. *Operation Security* adalah Keamanan Informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroprasi tanpa gangguan.
4. *Communication Security* adalah Keamanan Informasi bertujuan menggunakan media komunikasi, teknologi komunikasi, dan yang ada didalamya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. *Network Security* adalah keamanan informasi yang memfokuskan pada bagaimanan pengamanan peralatan jaringan, data organisasi, jaringanya dan

isinya, serta kemampuan untuk menggunakan jaringan tersebut dalalm memenuhi fungsi komunikasi data organisasi.

Aspek Keamanan Informasi meliputi tiga hal, yitu: *Confidentiality*, *Integrity*, dan *Availability* (*CIA*). Aspek tersebuut dapat dilihat pada Gambar 2.2 yang lebih lanjut akan di jelaskan sebagai berikut.

a) Kerahasiaan *(Confidentiality)*: Informasi bersifat rahasia dan harus dilindungi terhadap keterbuakaan dari pengguna yang tidak berkepentingan.
b) Ketersediaan *(Integrity)*: Layanan, fungsi sistem, informasi harus terjamin dan tersedia bagi pengguna saat diperlukan.
c) Integritas *(Availibility)*: Informasi harus komplit dan tidak dirubah. Dalam teknologi informasi, kata informasi terkait dengan berita. Hilangnya integritas informasi berarti berita tersebut tidak akurat.

Gambar 2.2 Aspek Keamanan Informasi
(Sumber: Sarno, 2009)

2.4 Pengembangan Multimedia Baru (PMB)

PMB merupakan bagian dari teknik studio dan media baru instansi penyiaran radio RRI Surabaya, sedangkan teknik studio dan multimedia baru merupakan unit dari stasuin penyiaran RRI Surabaya. PMB adalah bagian yang mendukung fasilitas dan kebutuhan penyiaran RRI wilayah Jawa Timur. Beberapa

kebutuhan di bagian penyiaran yaitu penyimpanan, pengelolaan berita, lagu, siaran, iklan, streaming, dan lain-lain untuk stasiun penyiaran kelas II RRI Surabaya.

2.5 Penilaian Risiko (*Risk Assessment*)

Penilaian risiko (*risk assessment*) adalah langkah atau tahap pertama dari proses manajemen risiko (Sarno dan Iffano, 2009). Penilaian risiko bertujuan untuk mengetahui ancaman-ancaman dari luar yang berpotensi mengganggu Keamanan Informasi organisasi dan potensial kelemahan yang dimiliki oleh Informasi organisasi. Metode penilaian risiko terdiri dari 6 tahapan, yaitu:

1. Identifikasi Informasi.
2. Identifikasi Ancaman (*threat*).
3. Identifikasi Kelemahan (*vulnerability*).
4. Menentukan Kemungkinan Ancaman (*probability*).
5. Analisa Dampak (*impact analysis*).
6. Menentukan Nilai Risiko.

Menurut (Sarno dan Iffano, 2009) nilai risiko (*risk value*) adalah Gambaran dari seberapa besar akibat yang akan diterima oleh organisasi jika ancaman (*threat*) yang menyebabkan kegagalan keamanan informasi terjadi. Dalam Tugas Akhir ini penilaian risiko menggunakan metode kuantitatif.

Metode kuantitatif adalah metode penilaian risiko dengan pendekatan matematis. Dengan metode ini nilai risiko dapat dihitung dengan menggunakan rumus berikut.

a) Menghitung nilai aset berdasarkan aspek keamanan informasi, yaitu: kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan

(*availability*). Nilai aset dihitung dengan menggunakan persamaan matematis berikut:

Nilai Aset = NC + NI + NV …….....(2.1)

Dimana:

NC = Nilai *Confidetiality* sesuai nilai yang dipilih Tabel.

NI = Nilai *Integrity* sesuai nilai yang dipilih pada Tabel.

NV = Nilai *Availability* sesuai nilai yang dipilih pada Tabel.

b) Mengidentifikasi ancaman dan kelemahan yang dimiliki oleh aset dapat dilakukan dengan membuat Tabel kemungkinan kejadian (*probability of occurrence*). Nilai rata-rata probabilitas dihasilkan dari klasifikasi probabilitas dengan rentang nilai yang dapat didefinisikan sebagai berikut:

Low **:** Nilai rata-rata probabilitas 0,1 - 0,3.

Medium **:** Nilai rata-rata probabilitas 0,4 - 0,6.

High **:** Nilai rata-rata probabilitas 0,7 - 1,0.

Nilai ancaman dari suatu aset dapat dihitung dengan rumus:

NT = ∑PO / ∑Ancaman ……..…(2.2)

Dimana:

∑PO : Jumlah *probability of occurrence*.

∑Ancaman : Jumlah ancaman terhadap informasi.

c) Analisa dampak bisnis (*Business Impact Analysis*) dapat diistilahkan dengan BIA. Menganalisa dampak bisnis dapat dilakukan dengan cara membuat skala nilai BIA. Dampak bisnis dibagai dalam lima level penilaian, yaitu:

$0 \geq$ *Not Critical Impact* ≤ 20

$20 >$ *Low Critical Impact* ≤ 40

40 > *Medium Critical Impact* ≤ 60

60 > *High Critical Impact* ≤ 80

80 > *Very High Critical Impact* ≤ 100

Mengidentifikasi level risiko dapat dilakukan dengan membuat Tabel level risiko. Didalam Tabel level risiko terdapat nilai ancaman yang dibagi dalam 3 level penilaian, yaitu:

0 ≥ *Low Probability* ≤ 0,1

0,1 > *Medium Probability* ≤ 0,5

0,5 > *High Probability* ≤ 1,0

d) Perhitungan nilai risiko dengan pendekatan matematis:

***Risk Value* = NA x BIA x NT** …….....…(2.3)

Dimana:

Nilai Aset: NA

Analisa Dampak Bisnis: BIA

Nilai Ancaman: NT

Menurut (Sarno dan Iffano, 2009) setelah menentukan metode penilaian risiko, maka organisasi harus menentukan bagaimana kriteria penerimaan risiko. Kriteria ini sebagai acuan tindakan apa yang akan dilakukan oleh organisasi dalam menerima risiko jika terjadi kegagalan Keamanan Informasi. Adapun kriteria penerimaan risiko dapat dikategorikan sebagai berikut.

1. Risiko Diterima (*risk acceptance*)

   Organisasi menerima risiko yang terjadi dengan segala dampaknya dan proses bisnis organisasi berlangsung terus.

2. Risiko Direduksi (*risk reduction*)

   Organisasi menerima risiko yang terjadi direduksi dengan menggunakan Kontrol Keamanan sampai pada level yang dapat diterima oleh organisasi.

3. Risiko Dihindari atau Ditolak (*risk avoidance*)

   Organisasi menghindari risiko yang terjadi dengan cara menghilangkan penyebab timbulnya risiko atau organisasi menghentikan aktivitasnya jika gejala risiko muncul (seperti: mematikan komputer *server*, memutus koneksi jaringan, dan lain-lain).

4. Risiko Dialihkan Pada Pihak Ketiga (*risk transfer*)

   Organisasi menerima risiko dengan cara mengalihkan pada pihak ketiga untuk mendapat penggantian atau kompensasi dari pihak ketiga (seperti kepada perusahaan asuransi, vendor, dan lain-lain).

Metode untuk menentukan kriteria penerimaan risiko dapat menggunakan Tabel matrik 3x3 dapat dilihat pada Tabel 2.2.

Tabel 2.2 Kriteria Penerimaan Risiko

Probabilitas Ancaman (PA)	**Biaya Pemulihan (BP)**		
	Low	***Medium***	***High***
High	*Risk Acceptance*	*Risk Avoidance*	*Risk Transfer*
Medium	*Risk Acceptance*	*Risk Reduction*	*Risk Transfer*
Low	*Risk Acceptance*	*Risk Reduction*	*Risk Transfer*
	High	***Medium***	***Low***
	Biaya Transfer Risiko (BR)		

(Sumber: Sarno dan Iffano, 2009)

Kriteria penerimaan risiko pada Tabel 2.2 diatas menggunakan prinsip logika penerimaan risiko AND serta dapat dijelaskan sebagai berikut:

1. Jika salah satu nilai variabel ber logika *Low* maka risiko diterima dan sebaliknya jika salah satu nilai variabel berlogika *High* maka risiko ditolak.

2. Kriteria risiko diterima dapat dikembangkan dengan kriteria tambahan yaitu:

    a. Jika biaya pemulihan **lebih kecil** daripada biaya transfer risiko, maka risiko diterima dengan status *risk acceptance*.

    b. Jika biaya pemulihan **lebih besar** daripada biaya transfer risiko, maka risiko diterima dengan status *risk transfer*.

    c. Jika biaya pemulihan **sama** dengan biaya transfer risiko, maka risiko diterima dengan status *risk reduction*, yaitu risiko direduksi dengan menggunakan pengendalian Kontrol Keamanan sampai pada level yang dapat diterima oleh organisasi, kecuali jika probabilitas ancaman bernilai *HIGH* maka risiko ditolak.

2.6 Standar Sistem Manajemen Keamanan Informasi

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

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

   Dokumen definisi-definisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.

b. ISO/IEC 27001:2005-*ISMS Requirements*

   Berisi persyaratan standar yang harus dipenuhi untuk membangun SMKI.

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

Terkait dengan dokumen ISO 27001, namun dalam dokumen ini berisi panduan praktis (*code of practice*) teknik keamanan informasi.

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

Berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

e. ISO/IEC 27004:2009-*ISMS Measurements*

Berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

f. ISO/IEC 27005:2008-*Infromation Security Risk Management*

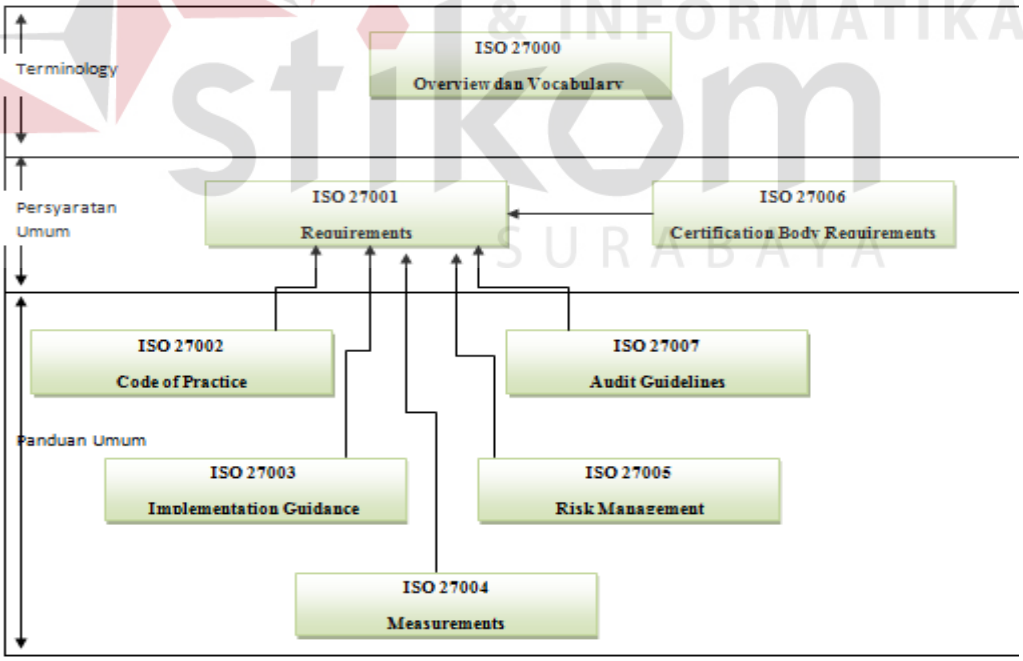
Dokumen panduan pelaksanaan manajemen resiko.

g. ISO/IEC 27006:2007-ISMS *Certification Body Requirements*

Dokumen panduan untuk sertifikasi SMKI perusahaan.

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

Dokumen panduan audit SMKI perusahaan.



Gambar 2.3 Relasi Antar Keluarga Standar SMKI
(Sumber: Sarno dan Iffano, 2009)

Dokumen panduan audit SMKI perusahaan. Adapun penjelasan dari standar ISMS tersebut dijelaskan sebagai berikut.

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

Standar ini dirilis tahun 2009, memuatprinsip-prinsip dasar *Information Security Management System*, definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga SMKI, baik yang telah diterbitkan maupun sedang tahap pengembangan. Hubungan antar standar keluarga ISO 27000 dapat dilihat pada Gambar 2.3.

b. SNI ISO/IEC 27001- Persyaratan Sistem Manajemen Keamanan Informasi

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

Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoprasian, pemantauan, tinjau ulang (*review*), pemeliharaan dan peningkatan suatu SMKI. Model *PLAN, DO, CHECK, ACT* (PDCA) diterapkan terhadap struktur keseluruhan proses SMKI. Dalam model PDCA, keseluruhan proses SMKI dapat dipetakan seperti Tabel 2.3.

Tabel 2.3 Peta PDCA dalam proses SMKI

PLAN (Menetapkan SMKI)	Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola resiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dari sasaran

Tabel 2.3 (Lanjutan)

DO (Menerapkan dan mengoperasikan 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 meningkatkan SMKI)	Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

(Sumber: Sarno dan Iffano, 2009)

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

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

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

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

e. ISO/IEC 27004:2009 – *Information Security ManagementMeasurement*

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

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

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

g. ISO/IEC 27006:2007 – Prasyarat Badan Audit dan Sertifikasi

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

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

Standar ini memaparkan panduan bagaimana melakukan audit SMKI perusahaan.

2.7 ISO/IEC 27002:2005 – Code of Practice for ISMS

Seperti yang telah dikemukakan pada bagian terdahulu, ISO/IEC 27002:2005 terkait dengan dokumen ISO 27001, namun dalam dokumen ini berisi panduan praktis (*code of practice*) teknik keamanan informasi. Kontrol keamanan berdasarkan ISO/IEC 27002 terdiri dari 12 klausul kontrol keamanan (*security*

control clauses), 41 objektif kontrol (*control objectives*) dan 133 kontrol keamanan/ kontrol (*controls*) yang dapat dilihat dalam Tabel 2.3.

Tabel 2.3 Ringkasan Jumlah Klausul Kontrol Keamanan, Objektif Kontrol dan Kontrol

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

(Sumber: Sarno, 2009)

ISO 27002:2005 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 12 area pengamanan sebagaimana ditetapkan didalam ISO/IEC 27002.

Dalam penelitian ini, audit keamanan sistem informasi akan difokuskan pada standar 3 klausul, yaitu klausul 8 tentang keamanan sumber daya manusia, klausul 9 tentang keamanan fisik dan lingkungan, klausul 11 tentang kontrol akses yang sudah disesuaikan dengan kesepakatan auditor dan Kepala Seksi PMB dalam *engagement letter* surat perjanjian audit, untuk detail struktur dokumen kontrol keamanan dari ISO/IEC 27002:2005 dapat dilihat pada Tabel 2.4.

Tabel 2.4 Detail Struktur Kontrol Acuan Audit Keamanan Informasi ISO/IEC 27002:2005

Klausul: 8 Keamanan Sumber Daya Manusia		
Kategori Keamanan Utama: *8.1 Sebelum menjadi pegawai* *Objektif Kontrol:* Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga memahami akan tanggung jawabnya dan bisa menjalankan aturan yang mereka dapatkan untuk meminimalkan resiko pencurian atau kesalahan dalam penggunaan fasilitas informasi.		
8.1.1	Aturan dan tanggung jawab keamanan	*Kontrol:* Aturan-aturan dan tanggung jawab dari pegawai, kontraktor dan pengguna pihak ketiga harus didefinisikan, didokumentasi sesuai dengan kebijakan Keamanan Informasi organisasi.
Kategori Keamanan Utama: *8.2 Selama menjadi pegawai* *Objektif Kontrol:* Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga memahami Keamanan Informasi yang telah ditetapkan oleh organisasi demi mengurangi terjadinya kesalahan kerja (*human error*) dan resiko yang dihadapi oleh organisasi.		
8.2.1	Tanggung jawab manajemen	*Kontrol:* Manajemen harus mensyaratkan seluruh pegawai, kontraktor atau pihak ketiga untuk mengaplikasikan Keamanan Informasi sesuai dengan kebijakan dan prosedur Keamanan Informasi yang telah dibangun

Tabel 2.4 (Lanjutan).

Kategori Keamanan Utama: *8.2 Selama bekerja*		
Objektif Kontrol: Untuk memastikan bahwa keamanan diterapkan dalam pekerjaan seluruh individu di organisasi.		
8.2.2	Pendidikan dan pelatihan keamanan informasi	*Kontrol:* Seluruh pegawai di dalam organisasi, kontraktor atau pihak ketiga yang relevan harus mendapat pelatihan yang cukup relevan sesuai diskripsi kerja masing-masing tentang kepedulian Keamanan Informasi. Hal ini dilakukan secara regular sesuai dengan perubahan kebijakan dan prosedur di organisasi.
Klausul: 9 Keamanan fisik dan lingkungan		
Kategori Keamanan Utama: 9*.1 Wilayah aman* *Objektif Kontrol:* Untuk mencegah akses fisik tanpa hak, kerusakan dan ganguan terhadap Informasi dan perangkatnya dalam organisasi.		
9.1.2	Kontrol masuk fisik	*Kontrol:* Wilayah aman (*secure*) harus dilindungi dengan kontrol akses masuk yang memadai untuk memastikan hanya orang yang berhak saja-dibolehkan masuk.

Klausul: 9 Keamanan fisik dan lingkungan		
Kategori Keamanan Utama: 9*.1 Wilayah aman* *Objektif Kontrol:* Untuk mencegah akses fisik tanpa hak, kerusakan dan ganguan terhadap Informasi dan perangkatnya dalam organisasi.		
9.1.3	Keamanan kantor, ruang dan fasilitasnya	*Kontrol:* Keamanan fisik untuk kantor, ruang dan fasilitasnya harus disediakan dan diimplementasikan.

Tabel 2.4 (Lanjutan)

Kategori Keamanan Utama: 9.*2 Keamanan Peralatan*		
Objektif Kontrol: Untuk mencegah kehilangan, kerusakan, pencurian atau ketidakberesan aset dan gangguan terhadap aktivitas organisasi.		
9.2.1	Letak peralatan dan pengamanannya	*Kontrol:* Semua peralatan harus ditempatkan dengan tepat dan dilindungi untuk mengurangi resiko dari ancaman dan bahaya dari lingkungan sekitar atau kesempatan untuk diakses dari orang- orang yang tidak berhak.
9.2.3	Keamanan pengkabelan	*Kontrol:* Kabel daya dan telekomunikasi yang menyalurkan data dan layanan Informasi harus dilindungi dari gangguan dan kerusakan.

2.8 Tingkat Kematangan (CMMI) to ISO 27002

Dimensi kematangan *Capability Maturity Model Integration* (CMMI) digunakan untuk kegiatan *benchmarking* dan penilaian, tingkat kematangan berlaku untuk pencapaian proses perbaikan organisasi (CMMI-DEV V1.3, 2010).

Tabel 2.5 CMMI to ISO 27002

Level	***Continous Representation Capability Levels***	***Staged Representation Maturity Levels***
0	***Incomplete***	
1	***Performed***	***Initial***
2	***Managed***	***Managed***
3	***Defined***	***Defined***
4		***Quantitatively Managed***
5		***Optimizing***

(Sumber: CMMI-DEV V1.3, 2010)

Tingkat kematangan organisasi pada Tabel 2.5 menyediakan cara untuk mengkarakterisasi kinerjanya. Pengalaman menunjukkan bahwa organisasi melakukan yang terbaik ketika mereka memfokuskan upaya perbaikan proses

mereka pada sejumlah proses yang dikelola. Sebuah tingkat kematangan adalah dataran tinggi evolusi yang ditetapkan untuk perbaikan proses organisasi. Setiap tingkat kematangan organisasi sangat penting untuk mempersiapkan perpindahan ke tingkat kematangan berikutnya (CMMI-DEV V1.3, 2010).

1. Tingkat Kematangan Level 1: *Initial*

   Pada tingkat kematangan level 1, proses organisasi masih kacau. Organisasi tidak menyediakan lingkungan yang stabil untuk mendukung proses. Organisasi dapat sukses tergantung dari kompetensi dan orang-orang di dalam organisasi, bukan dari penggunaan proses. Pada level ini, organisasi ditandai dengan kecenderungan untuk *overcommit*, meninggalkan proses mereka dalam waktu krisis, dan tidak dapat mengulangi keberhasilan mereka.

2. Tingkat Kematangan Level 2: *Managed*

   Pada tingkat kematangan level 2, telah dipastikan bahwa proses proyek sudah direncanakan dan dilaksanakan dengan dokumentasi yang terbatas. Memperkerjakan sumber daya yang terampil untuk menghasilkan *output* yang dapat dikendalikan, melibatkan *stakeholder* terkait monitoring, pengendalian, peninjauan, dan proses evaluasi untuk kepatuhan terhadap deskripsi proses. Komitmen telah ditetapkan antar pemangku kepentingan dan direvisi sesuai dengan kebutuhan. Produk dan layanan pekerjaan ditentukan sesuai deskripsi proses, standar, dan prosedur mereka.

3. Tingkat Kematangan Level 3: *Defined*

   Pada tingkat kematangan level 3, proses sudah dipahami dengan baik, dijelaskan dalam standar, prosedur, alat, dan metode. Kumpulan proses

organisasi merupakan dasar level 3 agar dapat ditingkatkan dari waktu ke waktu. Pada tingkatan level 2 deskripsi proses dan prosedur bisa sangat berbeda dengan level 3 yang lebih dijelaskan secara detil. Sebuah proses pada level 3 didefinisikan dengan jelas meliputi tujuan, masukan, kriteria, kegiatan, peran, langkah-langkah, verifikasi, dan hasil. Pada tingkat kematangan level 3, proses dikelola lebih proaktif menggunakan pemahaman tentang hubungan timbal balik dari kegiatan, langkah-langkah, produk kerja, dan layanannya.

4. Tingkat Kematangan Level 4: *Quantitatively Managed*

   Pada tingkat kematangan level 4, organisasi dan proyek menerapkan tujuan kuantitatif untuk kualitas dan kinerja proses digunakan sebagai kriteria pengelolaan proyek. Tujuan kuantitatif didasarkan pada kebutuhan pelanggan, pengguna akhir, organisasi, dan pelaksana proses. Kualitas dan kinerja proses dipahami serta dikelola selama proyek berlangsung. Untuk subproses yang dipilih, langkah-langkah khusus dari kinerja proses dikumpulkan dan dianalisis secara statistik. Ketika memilih subproses untuk analisis, sangat penting untuk memahami hubungan antara subproses yang berbeda dan dampaknya terhadap pencapaian tujuan untuk kualitas dan kinerja proses. Pendekatan statistik membantu untuk memastikan bahwa pemantauan subproses menggunakan teknik kuantitatif statistik diterapkan agar memiliki nilai yang paling baik untuk bisnis. Perbedaan penting antara tingkat kematangan 3 dan 4 adalah prediktabilitas kinerja proses. Pada tingkat kematangan 4, kinerja proyek dan subproses yang dipilih dikendalikan menggunakan teknik kuantitatif statistik dan prediksi didasarkan pada sebagian data proses analisis statistik.

5. Tingkat Kematangan Level 5: *Optimizing*

Pada tingkat kematangan level 5, sebuah organisasi terus-menerus meningkatkan proses yang didasarkan pada pemahaman kuantitatif tujuan bisnis dan kebutuhan kinerja. Organisasi menggunakan pendekatan kuantitatif untuk memahami variasi yang melekat dalam proses dan penyebab hasil proses. Tingkat kematangan level 5 berfokus pada kinerja proses terus ditingkatkan secara bertahap disertai dengan perbaikan teknologi. Kualitas dan kinerja organisasi terus direvisi mencerminkan perubahan tujuan bisnis dan kinerja organisasi. Efek dari perbaikan proses diukur menggunakan teknik kuantitatif statistik dan dibandingkan dengan tujuan, kinerja, kualitas. Perbedaan penting antara tingkat kematangan 4 dan 5 adalah fokus pada pengelolaan dan meningkatkan kinerja organisasi. Pada tingkat kematangan 4, organisasi dan proyek fokus pada pemahaman dan mengendalikan kinerja di tingkat subproses dan menggunakan hasil untuk mengelola proyek. Pada tingkat kematangan 5, organisasi yang bersangkutan dengan kinerja organisasi secara keseluruhan menggunakan data yang dikumpulkan dari beberapa proyek. Analisis data mengidentifikasi kekurangan atau kesenjangan dalam kinerja. Kesenjangan ini digunakan untuk mendorong perbaikan proses organisasi yang menghasilkan peningkatan kinerja.