BAB II

LANDASAN TEORI

2.1 Audit

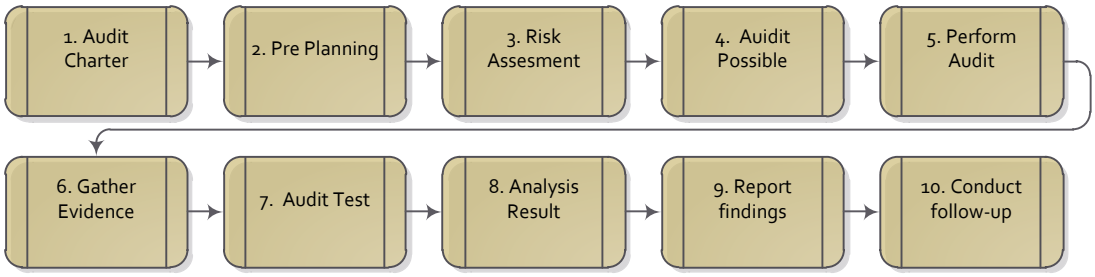
Penggunaan istilah audit telah banyak dipakai di berbagai disiplin ilmu, mulai dari keuangan, pemerintahan hingga Teknologi Informasi (TI). Adapun definisi audit menurut Sarno, R adalah:

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, 2009:171).

Dari pendapat R. Sarno diatas dapat disimpulkan bahwa audit mengandung arti aktivitas yang berlangsung secara sistematik atau terarah, independen atau mandiri dan terdokumentasi artinya ada rekam jejak, temuan atau bukti.

Selama audit penting untuk mengingat bahwa semua pendapat dan keputusan perlu di dukung bukti dan dokumentasi. Auditor harus bertanggung jawab dan memastikan kosistensi dalam proses audit tersebut. Adapun tahapan Audit berdasarkan (CISA, 2011), terdapat sepuluh (10) tahap yang dilakukan dalam proses audit, yaitu: 1. Membuat dan Mendapatkan Persetujuan Surat Keterikatan, 2. Perencanaan Audit, 3. Analisi Risiko. 4. Kemungkinan Audit, 5. Pelaksanaan Audit, 6. Pemeriksaan Data dan Bukti, 7. Tes Audit, 8. Pemeriksaan Hasil Audit,9. Pelaporan Audit, 10. Pertemuan Penutupan/ *Exit Meeting.*

Tahapan audit berdasarkan CISA dapat dilihat pada Gambar 2.1.



Gambar 2.1. Tahapan-tahapan Audit Teknologi Informasi
(Sumber: CISA, 2011)

1. Membuat dan Mendapatkan Persetujuan E*ngagement Letter*

Sebelum melakukan audit, seorang auditor harus membuat surat kesepakatan atau keterikatan dengan *client* untuk berkomitmen menjaga dan mentaati persetujuan dan peraturan yang telah dibuat selama audit dilakukan. Surat atau perjanjian yang dibuat oleh auditor internal dinamakan *audit charter* sedangkan untuk auditor eksternal dinamakan *engagement letter*. *Engagement letter* adalah surat yang dikirimkan pada *client* pada awal permulaan audit yang didalamnya terdapat kontrak untuk menghindari kesalahpahaman antara klien dan auditor. Pada *engagement letter* didalamnya terdapat enam (6) point, yaitu:

1. Tanggung jawab
2. Wewenang
3. Tujuan
4. Peran
5. Objek audit
6. Waktu awal sampai akhir audit

2. Perencanaan Audit

Auditor harus mengetahui tentang *auditee* (*know your auditee*) dan harus mampu mempelajari dokumen-dokumen organisasi, yaitu: profil, rencana strategis, prosedur, standar operasi, kebijakan, portofolio, arsitektur, infrastruktur, aplikasi sistem informasi dan laporan audit sebelumnya. Auditor melakukan *interview* manajemen dan staf dan observasi kegiatan operasional dan teknologi sistem informasi yang digunakan. Pelajari regulasi yang mempengarui proses bisnis.

3. Analisis Risiko

Setelah melakukan perencanaan auditor melakukan penilaian risiko TI untuk menentukan objek-objek TI mana yang perlu mendapatkan perhatian dan alokasi sumber daya audit yang lebih dibandingkan dengan objek-objek lainnya.

Teknik Penilaian Risiko TI

a. Judgemental

b. Numeric rating

c. Combination of judgemental and numeric rating

4. Penentuan apakah audit dimungkinkan

Auditor harus bertanggung jawab dalam pelaksanaan audit. Penetapan objek audit TI dan skala prioritasnya dilakukan berdasarkan hasil penilaian risiko yang telah dilakukan sebelumnya. Objek audit TI yang beresiko tinggi harus memperoleh prioritas yang lebih tinggi dari objek audit yang beresiko lebih rendah. Auditor harus bekerjasama dengan *auditee* dalam melakukan audit, audit tanpa bukti berati audit tersebut sia-sia atau tidak berguna.

5. Pelaksanaan Audit

Sebelum melakukan atau melaksanakan audit seorang auditor akan melakukan persiapan. Terdapat beberapa langkah dalam tahap persiapan audit, yaitu:

a. Melakukan Pertemuan Pendahuluan Audit TI

Pertemuan pendahuluan dilakukan untuk:

1. Mendapatkan pemahaman yang sama atas audit TI yang akan dilakukan
2. Mendapatkan penjelasan dari pemimpin auditee tentang kondisi terakhir

objek audit dan hal-hal yang perlu menjadi perhatian. Pertemuan pendahuluan didokumentasikan dalam bentuk risalah/ notulen pertemuan pendahuluan.

b. Penyampaian Surat Penugasan

Tim auditor TI dalam setiap melaksanakan tugasnya harus berdasarkan surat penugasan yang ditanda tangani oleh kepala direksi. Surat penugasan merupakan bentuk pendelegasian wewenang kepala kepada tim auditor TI untuk melaksanakan audit.

c. Koordinasi Tim Auditor

Koordinasi perlu dilakukan agar setiap anggota tim auditor TI memahami tugas dan tanggung jawabnya secara jelas sesuai dengan AWP yang telah disusun sebelumnya oleh ketua tim auditor sehingga audit dapat:

1. Dilaksanakan secara efektif dan efisien
2. Mencapai tujuan yang telah ditetapkan
3. Memenuhi kebutuhan manajemen

d. Penyusunan Audit Working Plan (AWP)

Audit *Working Plan* merupakan dokumen yang dibuat oleh Ketua Tim Auditor TI yang digunakan untuk merencanakan dan memantau pelaksanaan Audit TI secara terperinci.

e. Penyampaian Kebutuhan Data

Data yang diperlukan Auditor TI dapat disampaikan terlebih dahulu kepada auditee agar dapat dipersiapakan terlebih dahulu. *Field Work* dilaksanakan auditor TI setelah *auditee* menginformasikan ketersediaan semua data yang diperlukan auditor TI, sehingaa *field work* dapat dilaksanakan oleh auditor TI secara efektif dan efisien.

f. Persiapan Kertas Kerja Audit

Auditor mempersiapkan kertas kerja audit TI yang didalmnya terdapat asmua dokumentasi proses audit TI yang dilakukan oleh. Contoh: AWP, Dokumen Administrasi Audit TI, Program Audit TI beserta kertas kerja pendukungnya, Form analisa data *interview*, observasi, data dan bukti audit, daftar temuan dan laporan audit.

Setelah persiapan telah dilakuan selanjutnya Audit dapat dilaksanakan. Pelaksanaan Audit terdapat beberapa langkah, yaitu:

a. Penyusunan Daftar Temuan

Daftar Temuan disampaikan secara lugas dan objektif dilengkapi dengan:

1. Deskripsi / penjelasan singkat dari temuan yang diungkap
2. Kriteria (peraturan, standar dan praktik terbaik yang menjadi acuan)
3. Risiko-risiko yang mungkin timbul jika temuan tidak ditindaklanjuti
4. Rekomendasi dari auditor TI yang perlu ditindaklanjuti oleh auditee agar Risiko - risiko yang ada tidak terjadi.

5. Harus didukung data, bukti, dan fakta yang benar
6. Mengacu pada kriteria yang relevan dengan kebutuhan dan kewajiban *auditee* dan telah ditetapkan menjadi acuan pelaksanaan audit TI

b. Konfirmasi Temuan

Temuan harus dikonfirmasikan terlebih dahulu kepada *auditee* sebelum dilaporkan secara formal (Kepada Bidang dan Sekertaris) dalam bentuk laporan TI. Konfirmasi temuan didokumentasikan dalam bentuk risalah / konfirmasi temuan.

6. Melakukan Pemeriksaan Data dan Bukti

Setiap langkah pemeriksaan yang ada dalam program audit dilaksanakan oleh auditor TI dengan menggunakan satu atau lebih teknik audit yang sesuai dan disertai data /bukti pendukung yang memadai / mencukupi.

7. Melakukan Tes Audit

Pemeriksaan data dan bukti dapat dilakukan melalui 2 tahap tes, yaitu:

1. *Compliance* tes: Pengujian untuk mengetahui keberadaaan/ penerapan pengendalian dalam kegiatan operasional objek audit
2. *Substantive* tes: Pengujian memastikan kelengkapan, integritas, dan keakuratan (kebenaran dan kekonsitenan) data dan informasi

Dalam melakukan tes audit terdapat beberapa teknik yaitu:

a) Teknik *review*: pemeriksaan ulang terhadap dokumentasi dan konfigurasi TI. Contoh: Dengan memeriksa ulang kelengkapan dan kepatuhan dalam pelaksanaan kebijakan, standar dan prosedur TI dan memeriksa kelengkapan dan pengembangan staf yang ada dalam struktur organisasi TI.

b) Teknik *interview*: pemeriksaan secara langsung terhadap *brainware* yang menjadi pengelola dan pengguna IT organisasi.

Contoh: *interview* terhadap pengelola departemen terkait dengan kegiatan operasional pemeliharaan dan pengaman dan interview terhadap pengguna TI terkait dengan kepuasan terhadap ketersediaan layanan IT.

c) Teknik *Observation*: Pemeriksaan secara langsung pada operasional objek TI.

Contoh: meninjau dan memeriksa infrastruktur kelistrikan, pengaturan udara dan pengaman ruang. Ikut serta dan mengamati pegguna dalam menggunakan aplikasi untuk mendukung kegiatan operasional sehari-hari. Meninjau dan memeriksa *software-software* yang terinstall di dalam komputer-komputer *client*.

d) *Trial* tes: Menguji secara langsung fungsI perangkat TI untuk mengetahui kelayakan dan kinerja operasionalnya.

Contoh: menguji fungsi sistem pendeteksi dan pemadam kebakaran (*fire suppression system*), mematikan aliran listrik ke komputer untuk menguji fungsi UPS dan genset.

8. Pemeriksaan Hasil Audit

Setiap langkah pemeriksaan yang ada dalam Program Audit dilaksanakan oleh Auditor TI dengan menggunakan satu atau lebih Teknik Audit yang sesuai dan dengan disertai data / bukti pendukung yang memadai / mencukupi.

9. Pelaporan Audit

Setelah Audit dilaksanakan auditor akan membuat laporan terdapat beberapa tahapan dalam pembuatan laporan, tahapan tersebut yaitu:

a. Penyusunan Laporan Audit TI

Berdasarkan seluruh kertas kerja audit, temuan dan tanggapan *auditee*, auditor TI harus menyusun draft laporan audit TI sebagai peratanggungjawaban atas penugasan audit TI yang telah dilaksanakan. Laporan audit TI ditujujan kepada pihak berhak saja karena laporan audit TI merupakan dokumen yang bersifat rahasia.

Isi (Draft) Laporan Audit TI:

1. Laporan Audit
    a. Penerima laporan
    b. Opini laporan
    c. Standar pelaksanaan audit yang dipergunakan
2. Ringkasan Eksekutif
    a. Periode audit TI
    b. Tanggal pelaksanaan audit TI
    c. Ringkasan hasil pemeriksaan TI
3. Pendahuluan
        A. Dasar pelaksanaan audit TI
        B. Tujuan audit TI
        C. Ruang lingkup audit
        D. Priode pemeriksaan
4. Metode pemeriksaan
5. Daftar Temuan
6. Lampiran

b. Permintaan Tanggapan Atas Temuan

Atas temuan yang telah disampaikan Auditor TI, Auditee harus memberikan tanggapan dan komitmen penyelesaiannya. Tanggapan secara formal atas setiap temuan Audit TI.

c. Persetujuan Laporan Audit TI

Draft laporan audit TI yang telah disusun harus dimintakan persetujuan terlebih dahulu kepada *auditee* sebelum dterbitkan sebagai laporan audit TI yang resmi dan formal. Persetujuan harus dilakukan oleh pejabat dii tingkat atas yang memadai (minimal Kepala Divisi TI).

10. Pertemuan Penutupan Audit

Pertemuan Penutup Audit TI dilakukan untuk melaporkan hasil audit TI kepada manjemen, memberikan penjelasan pada manajemen tentang kondisi kelemahan dan rekomendasi utama. Pertemuan di dokumentasikan dalam bentuk risalah/ Notulen pertemuan.

2.2 Sistem Informasi

Menurut Mukhtar (1999: 2), Sistem adalah suatu *entity* yang terdiri dari dua atau lebih komponen yang saling berinteraksi untuk mencapai tujuan. Sedangkan menurut James Hall dalam bukunya yang diterjemahkan oleh Jusuf (2001: 5), 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: 106)

Menurut Mukhtar (1999: 1), Informasi berarti hasil suatu proses yang terorganisasi, memiliki arti dan berguna bagi orang yang menerimanya. Adapun menurut James Hall pada bukunya (diterjemahkan oleh Amir Abadi Jusuf, 2001: 14): Informasi menyebabkan pemakai melakukan suatu tindakan yang dapat ia

lakukan atau tidak dilakukan. Informasi ditentukan oleh efeknya pada pemakai, bukan oleh bentuk fisiknya. (Gondodiyoto, 2007: 110)

Dengan demikian sistem informasi dapat didefinisikan sebagai kumpulan elemen-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: 112)

2.3 Audit Keamanan Sistem Informasi

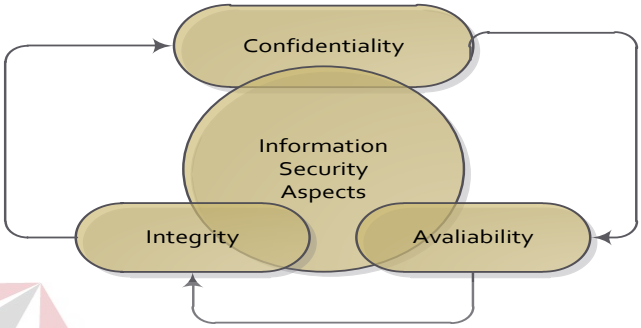
Di sisi lain kita juga mengenal istilah audit keamanan**,** adapun yang dimaksud dengan audit keamanan adalah suatu proses atau kejadian yang memiliki basis pada kebijakan atau standar keamanan untuk menentukan semua keadaan dari perlindungan yang ada, dan untuk mem*verifikasi* apakah perlindungan yang ada berjalan dengan baik. (Ahmad, 2012: 27)

Dari pengertian diatas dapat di garis bawahi bahwa audit keamanan tujuan utamanya adalah memberikan perlindungan sesuai dengan kebijakan dan standar keamanan yang ada serta memverifikasi apakah perlindungan sudah berjalan dengan baik. Oleh karena itu, suatu hal yang penting untuk memahami dan mengimplementasikan audit keamanan pada sistem informasi yang digunakan. Penerapan audit keamanan sistem informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun *non teknis*. Terdapat tiga kriteria mendasar dari keamanan teknologi informasi yang harus diaudit kemanannya menurut (Ahmad, 2012: 4), yaitu:

a. **Kerahasiaan *(confidentiality)*:** Informasi bersifat rahasia dan harus dilindungi terhadap keterbukaan dari yang tidak berhak atau berkepentingan.

b. **Ketersediaan *(availability)*:** Layanan, fungsi sistem teknologi informasi, data dan informasi harus tersedia bagi penggunaa saat diperlukan.

c. **Integritas *(integrity)*:** Data harus komplit dan tidak diubah. Dalam teknologi informasi, kata informasi terkait dengan data. Hilangnya integritas informasi berarti data tersebut telah tanpa adanya ijin atau ilegal.



Gambar 2.2 Aspek Keamanan Informasi
(Sumber: Sarno, 2009: 37)

2.4 Standar Sistem Manajemen Keamanan Informasi

Selama 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:

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

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

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

Berisi persyaratan standar yang harus dipenuhi untuk membangun SMKI.

f. 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.

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

Berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

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

Berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.

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

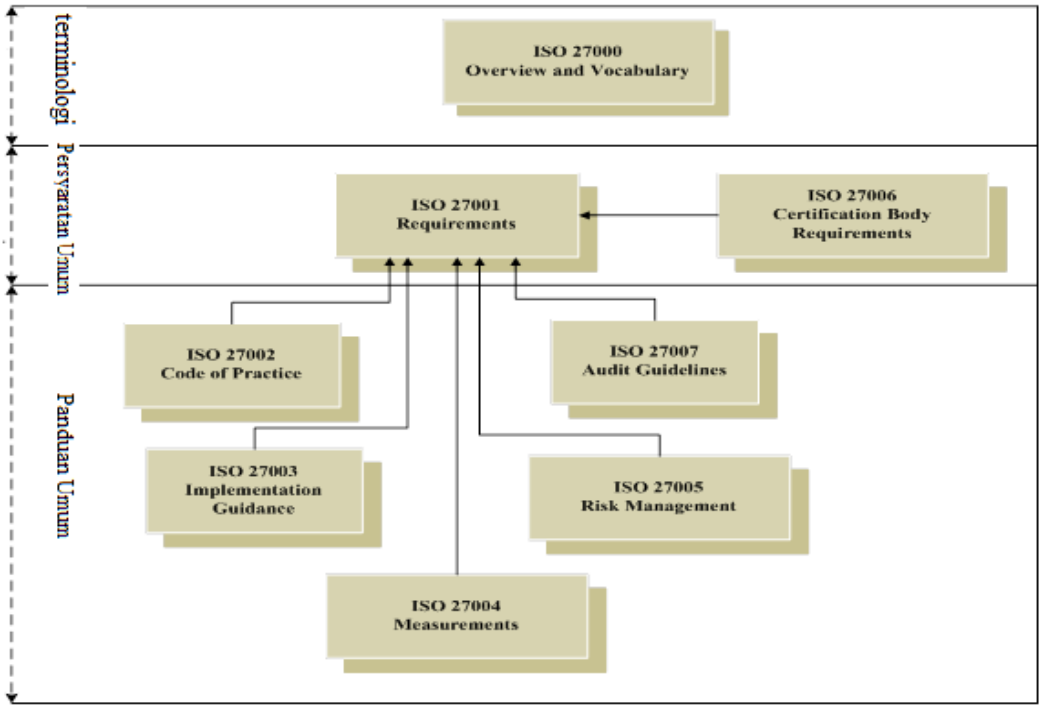
Dokumen panduan pelaksanaan manajemen resiko.

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

Dokumen panduan untuk sertifikasi SMKI perusahaan.

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

Dokumen panduan audit SMKI perusahaan.



Gambar 2.3 Relasi Antar Keluarga Standar SMKI
(Sumber Ahmad, 2012: 13)

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 2.1.

Tabel 2.1 Peta PDCA dalam proses SMKI

TABLE PETA PDCA 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
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:Ahmad, 2012: 15)

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.

2.5 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 11 klausul kontrol keamanan (*security control clauses*), 39 objektif kontrol (*control objectives*) dan 133 kontrol keamanan/ kontrol (*controls*) yang dapat dilihat dalam Tabel 2.2.

Tabel 2.2 Ringkasan jumlah klausul kontrol keamanan, objektif kontrol dan kontrol

Klausul	Jumlah	
	Objektif Kontrol	Kontrol
5	1	2
6	2	11
7	2	5
8	3	9
9	2	13
10	10	31
11	7	25
12	6	16
13	2	5
14	1	5
15	3	10
Jumlah : 11	Jumlah : 39	Jumlah : 133

(Sumber: Sarno, 2009: 187)

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 11 area pengamanan sebagaimana ditetapkan didalam ISO/IEC 27002.

Dalam penelitian ini audit keamanan sistem informasi akan difokuskan pada standar 3 klausul yang sudah disesuaikan dengan kesepakatan auditor dan kepala bagian DPPKD dalam *engagement letter*/ surat perjanjian audit, untuk detail struktur dokumen kontrol keamanan dari ISO/IEC 27002:2005 dapat dilihat pada Tabel 2.3.

Tabel 2.3 Detail Struktur Dokumen Kontrol Keamanan 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.
Kategori Keamanan Utama: *8.3 Pemberhentian atau pemindahan pegawai* *Objektif Kontrol:* Untuk memastikan bahwa pegawai, kontraktor atau pihak ketiga yang diberhentikan atau dipindah dilakukan sesuai prosedur yang benar.		
8.3.1	Tanggung jawab pemberhentian	*Kontrol:* Tanggung jawab terhadap pemberhentian atau pemindahan pegawai, kontraktor atau pihak ketiga harus didefinisikan dan ditunjuk dengan jelas.

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.
9.1.3	Keamanan kantor, ruang dan fasilitasnya	*Kontrol:* Keamanan fisik untuk kantor, ruang dan fasilitasnya harus disediakan dan diimplementasikan.

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.

Klausul: 11 Kontrol Akses		
Kategori Keamanan Utama: *11.1 Persyaratan bisnis untuk akses control* *Objektif Kontrol:* Untuk mengontrol akses Infromasi.		
11.1.1	Kebijakan kontrol akses	*Kontrol:* Suatu kebijakan kontrol akses harus dibuat, didokumentasikan dan dikaji ulang berdasarkan kebutuhan bisnisdan keamanan untuk akses.
Kategori Keamanan Utama: *11.2 Manajemen akses user* *Objektif Kontrol:* Untuk memastikan pengguna yang mempunyai hak akses ke Sistem Informasi dan yang tidak.		
11.2.3	Manajemen *password* user	*Kontrol:* Suatu kebijakan kontrol akses harus dibuat,

		didokumentasikan dan dikaji ulang berdasarkan kebutuhan bisnisdan keamanan untuk akses.
11.2.4	Tinjauan terhadap hak akses user	*Kontrol:* Suatu kebijakan kontrol akses harus dibuat, didokumentasikan dan dikaji ulang berdasarkan kebutuhan bisnisdan keamanan untuk akses.Manajemen harus melakukan tinjauan ulang terhadap hak akses user secara berkala melalui proses yang formal.
Kategori Keamanan Utama: *11.3 Tanggung jawab pengguna (user)* *Objektif Kontrol:* Untuk mencegah akses user tanpa hak atau pencurian Informasi dan fasilitas pemrosesan Informasi		
11.3.1	Penggunaan Password	*Kontrol:* Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan password.
Kategori Keamanan Utama: *11.4 Kontrol Akses jaringan* *Objektif Kontrol:* Untuk mencegah akses tanpa hak ke dalam layanan jaringan		
11.4.1	Kebijakan penggunaan layanan jaringan	*Kontrol:* Pengguna seharusnya hanya disediakan akses terhadaplayanan yang telah secara spesifik diotorifikasi dalam penggunaannya.
Kategori Keamanan Utama: *11.5 Kontrol Akses Sistem Operasi* *Objektif Kontrol:* Untuk mencegah akses tanpa hak ke sistem operasi.		
11.5.3	Sistem Manajemen Password	*Kontrol:* Sistem yang digunakan untuk mengelola

		password harus interaktif dan harus dipastikan passwordnya berkualitas.
Kategori Keamanan Utama: *11.6 Kontrol Akses Informasi dan aplikasi* *Objektif Kontrol:* Untuk mencegah akses tanpa hak terhadap Informasi yang terdapat di dalam aplikasi.		
11.6.1	Pembatasan akses Informasi	*Kontrol:* Akses terhadap Informasi dan sistem aplikasi oleh pengguna harus dibatasi sesuai dengan kebijakan keamanan yang ditentukan.
Kategori Keamanan Utama: *11.7 Komputasi bergerak dan bekerja dari lain tempat (teleworking)* *Objektif Kontrol:* Untuk memastikan Keamanan Informasi saat menggunakan fasilitas komputasi bergerak atau bekerja darilaintempat.		
11.7.1	Komunikasi dan terkomputerisasi yang bergerak	*Kontrol:* Kebijakan secara formal seharusnya ditempatkan dan pengukuran keamanan yang sesuai seharusnya diadopsi untuk melindungi resiko dari penggunaan fasilitas komunikasi dan komputer yang bergerak (*mobile computing and communication*).
11.7.2	Teleworking	*Kontrol:* Kebijakan, rencana operasional dan prosedur seharusnya dikembangkan dengan diimplementasikan untuk aktifitas *teleworking*.