BAB II

LANDASAN TEORI

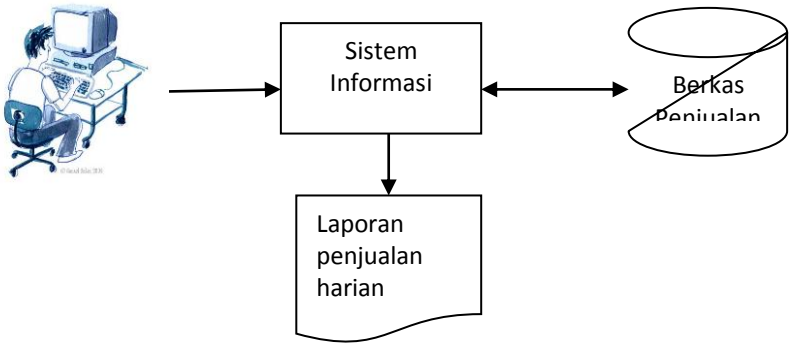
2.1 Sistem Informasi

Sistem informasi adalah kombinasi dari teknologi informasi dan aktivitas, yang menggunakan teknologi untuk mendukung kinerja, manajemen dan pembuatan keputusan (Beynon, 2004). Dalam hal ini, sistem informasi digunakan tidak hanya untuk menggambarkan komputer dan perangkatnya serta interaksinya dengan organisasi, tetapi juga digunakan untuk menggambarkan interaksi seluruh komponen yang terlibat dalam proses bisnis organisasi tersebut.

Berdasarkan definisi sistem informasi tersebut, menurut Kristanto (2003: 15-16) peranan sistem informasi dalam bisnis, antara lain:

1. Mendukung operasi bisnis
2. Mendukung dalam pengambilan keputusan manajerial
3. Meraih keuntungan strategik

Menurut Kadir (2003: 4) Sistem Informasi tidak harus selalu kompleks. Contoh sebuah sistem informasi yang sangat sederhana dapat dilihat pada Gambar 2.1 di halaman 9. Sistem tersebut hanya digunakan untuk mencatat transaksi penjualan dan melibatkan satu orang saja. Melalui sebuah komputer, pemakai memasukkan data penjualan dan saat setelah toko ditutup, laporan penjualan harian dicetak. Selanjutnya, laporan digunakan untuk melakukan analisis tentang barang-barang yang laku, yang berguna untuk pengambilan keputusan pembelian barang.



Gambar 2.1 Sistem Informasi yang Sederhana
(Sumber: Kadir, 2003: 4)

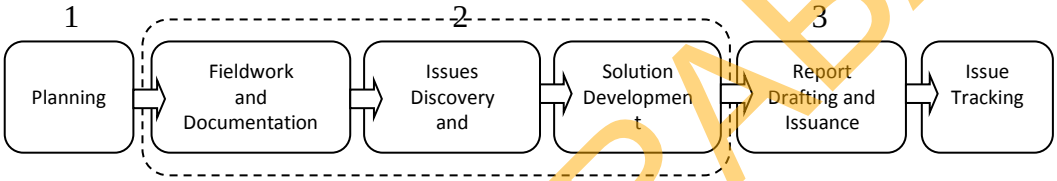
Sistem Informasi memberikan nilai tambah terhadap proses, produksi, kualitas, manajemen, pengambilan keputusan, dan pemecahan masalah serta keunggulan kompetitif yang tentu saja sangat berguna bagi kegiatan bisnis (Kroenke dalam Kadir, 2003: 5).

2.2 Audit

Definisi secara umum tentang audit adalah bahwa "*Auditing is an independent investigation of some particular activity*". Sebetulnya kata Audit itu sendiri berasal dari Bahasa Latin *Audire* yang dalam Bahasa Inggris berarti *to hear*. Makna yang dimaksud disini adalah "*hearing about the account's balances*" oleh para pihak terkait terhadap pihak ketiga yang netral (tidak ada *vested interest*) mengenai catatan keuangan perusahaan yang dikelola oleh orang-orang tertentu yang bukan sekaligus pemiliknya (Gondodiyoto, 2007: 28).

Menurut Susilo (2003: 80), audit adalah kegiatan mengumpulkan informasi faktual dan signifikan melalui interaksi (pemeriksaan, pengukuran dan penilaian yang berujung pada penarikan kesimpulan) secara sistematis, obyektif dan terdokumentasi yang berorientasi pada azas penggalian nilai atau manfaat.

Audit juga dapat didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokementasi untuk menemukan suatu bukti-bukti (audit *evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (ISACA, 2006).



Gambar 2.2 Audit *Process Overview*
(Sumber: Davis dkk, 2011: 43)

Davis, dkk, mendefinisikan tahapan audit dalam 6 (enam) tahapan yaitu *planning*, *fieldwork and documentation*, *issues discovery and validation*, *solution development*, *report drafting and issuance*, dan *issue tracking*, seperti yang tampak pada Gambar 2.2 Audit *Process Overview* yang setiap tahapan-tahapan yang dilakukan akan dijelaskan sebagai berikut.

1. *Planning*

Sebelum melaksanakan audit, sangat penting untuk menentukan rencana apa yang dilakukan untuk meninjau bagaimana audit dilakukan. Jika proses perencanaan dilakukan secara efektif, maka dapat membentuk tim audit yang dapat berjalan dengan baik. Sebaliknya, jika pekerjaan dimulai tanpa rencana yang jelas dan tanpa arah, upaya tim audit dapat mengakibatkan kegagalan.

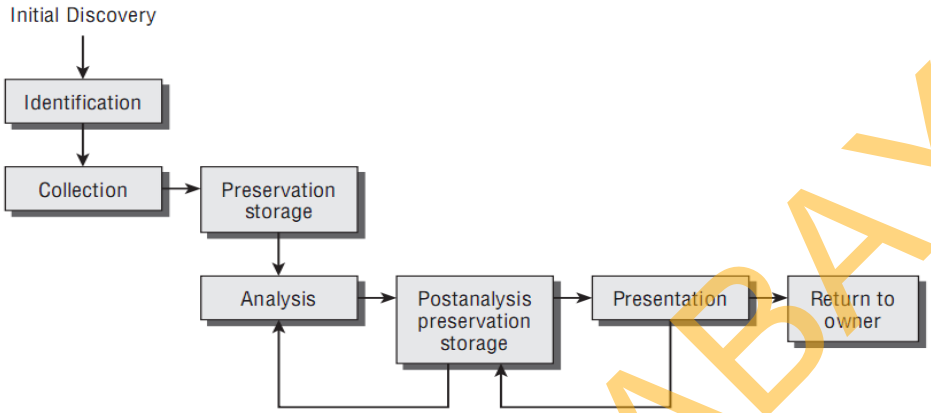
2. *Fieldwork and Documentation*

Fase ini adalah inti dalam proses audit dimana langkah-langkah audit yang telah dibuat selama tahap sebelumnya akan dijalankan oleh tim audit. Pada tahap ini tim audit telah memperoleh data dan melakukan wawancara yang akan membantu anggota tim ini untuk menganalisis data-data dan bukti-bukti yang ada. Auditor juga dituntut untuk dapat menguji berbagai hal dan melakukan pekerjaannya secara memadai baik melalui observasi maupun teknik-teknik audit yang lain. Selain itu, auditor mencari cara secara independen untuk melakukan validasi terhadap info yang diberikan dan menguji efektivitas pengendalian lingkungan. Selama melakukan audit, auditor harus dapat mendokumentasikan pekerjaan mereka sehingga kesimpulan dapat dibuktikan. Tujuan mendokumentasikan pekerjaan harus cukup detail sehingga cukup informasi bagi orang untuk dapat memahami apa yang telah dilakukan dan dapat mencapai kesimpulan yang sama seperti auditor. Tujuan dari tahapan ini adalah mengevaluasi keadaan kontrol internal di daerah yang sedang ditinjau.

3. *Issues Discovery and Validation*

Pada tahap ini auditor harus menentukan dan melakukan perbaikan pada daftar isu-isu yang potensial untuk memastikan isu-isu tersebut telah valid dan relevan. Auditor harus mendiskusikan isu-isu potensial dengan pelanggan secepat mungkin sebagai validasi terhadap keakuratan informasi dan kevalidan masalah yang ada. Selain melakukan validasi bahwa fakta-fakta yang ada telah benar, diperlukan juga melakukan validasi bahwa resiko yang disajikan oleh masalah ini cukup signifikan serta memiliki nilai untuk pelaporan dan pengalamatan. Menurut Cannon (2011: 187) temuan dan bukti-bukti yang ada harus dikonfirmasikan

terlebih dahulu kepada *auditee* sebelum dilaporkan secara formal kepada Direksi dalam bentuk laporan audit TI. Siklus hidup bukti temuan dapat dilihat pada Gambar 2.3.



Gambar 2.3 Siklus Hidup Bukti Temuan
(Sumber: Cannon, 2011: 187)

4. *Solution Development*

Setelah mengidentifikasi isu-isu potensial di wilayah yang sedang diaudit dan telah melakukan validasi fakta dan resiko yang ada, maka dapat dilakukan rencana untuk mengatasi setiap masalah tersebut. Dalam pengembangan solusi ini auditor harus fleksibel mengenai bagaimana menyelesaikan rencana tindakan harus dilakukan dalam laporan audit. Tiga pendekatan umum yang digunakan untuk mengembangkan tindakan dalam menangani masalah audit adalah 1. Pendekatan rekomendasi, 2. Pendekatan respon manajemen, dan 3. Pendekatan solusi.

Pendekatan apapun yang digunakan perusahaan, sangat penting menetapkan penanggung jawab untuk mengeksekusi rencana pelaksanaan dan tanggal jatuh tempo penyelesaiannya. Hal ini untuk kepentingan akuntabilitas dan sebagai dasar bagi auditor melakukan tindak lanjut.

5. *Report Drafting and Issuance*

Setelah ditemukan masalah dalam lingkungan yang diaudit, melakukan validasi, dan mengembangkankan solusi untuk mengatasi masalah yang ada, maka auditor dapat membuat draf laporan audit, yang merupakan dokumen hasil audit. Fungsi utama laporan audit adalah sebagai berikut.

a. Untuk auditor dan perusahaan yang diaudit, laporan audit berfungsi sebagai catatan audit, hasil audit, dan rencana rekomendasi yang dihasilkan.
b. Untuk manajemen senior dan komite audit, laporan audit berfungsi sebagai "kartu laporan" pada daerah yang telah diaudit.

6. *Issue Tracking*

Audit belum benar-benar lengkap sampai isu yang diangkat dalam audit tersebut diselesaikan. Departermen harus mengembangkan suatu proses di mana anggotanya dapat melacak dan mengevaluasi sampai isu terselesaikan. Auditor yang melakukan atau memimpin audit bertanggung jawab untuk menindaklanjuti poin dari audit seperti tanggal jatuh tempo untuk setiap pendekatan audit yang dilakukan.

2.3 Audit Sistem Informasi

Audit Sistem Informasi adalah proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif (Weber, 1999). Beberapa

elemen utama tinjauan penting dalam Audit Sistem Informasi yaitu dapat diklasifikasikan sebagai berikut.

1. Tinjauan terkait dengan fisik dan lingkungan, yakni: hal-hal yang terkait dengan keamanan fisik, suplai sumber daya, temperatur, kontrol kelembaban dan faktor lingkungan lain.
2. Tinjauan administrasi sistem, yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen database, seluruh prosedur administrasi sistem dan pelaksanaannya.
3. Tinjauan perangkat lunak. Perangkat lunak yang dimaksud merupakan aplikasi bisnis. Mencakup kontrol akses dan otorisasi ke dalam sistem, validasi dan penanganan kesalahan termasuk pengecualian dalam sistem serta aliran proses bisnis dalam perangkat lunak beserta kontrol secara manual dan prosedur penggunaannya. Sebagai tambahan, tinjauan juga perlu dilakukan terhadap siklus hidup pengembangan sistem.
4. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan 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 *backup* dan penyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana/kontinuitas bisnis yang dimiliki.
6. Tinjauan integritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

Tahapan audit sistem informasi dibagi menjadi 4 (empat) tahapan yaitu: 1. Tahap perencanaan audit, 2. Tahap persiapan audit, 3. Tahap pelaksanaan audit, 4. Tahap pelaporan audit (Hermawan, 2011). Keempat tahapan tersebut adalah sebagai berikut.

1. Tahap Perencanaan Audit Sistem Informasi

Tahap perencanaan ini dilakukan oleh auditor untuk mengetahui tentang *auditee* (*how your auditee*) dan mempelajari tentang proses bisnis perusahaan yang diaudit. Pada tahap ini ditentukan ruang lingkup dan tujuan dari audit sistem informasi yang hendak dikerjakan.

2. Tahap Persiapan Audit Sistem Informasi

Pada tahap persiapan, auditor merencanakan dan memantau pelaksanaan audit sistem informasi secara terperinci, kemudian mempersiapkan kertas kerja audit sistem informasi yang akan dipakai.

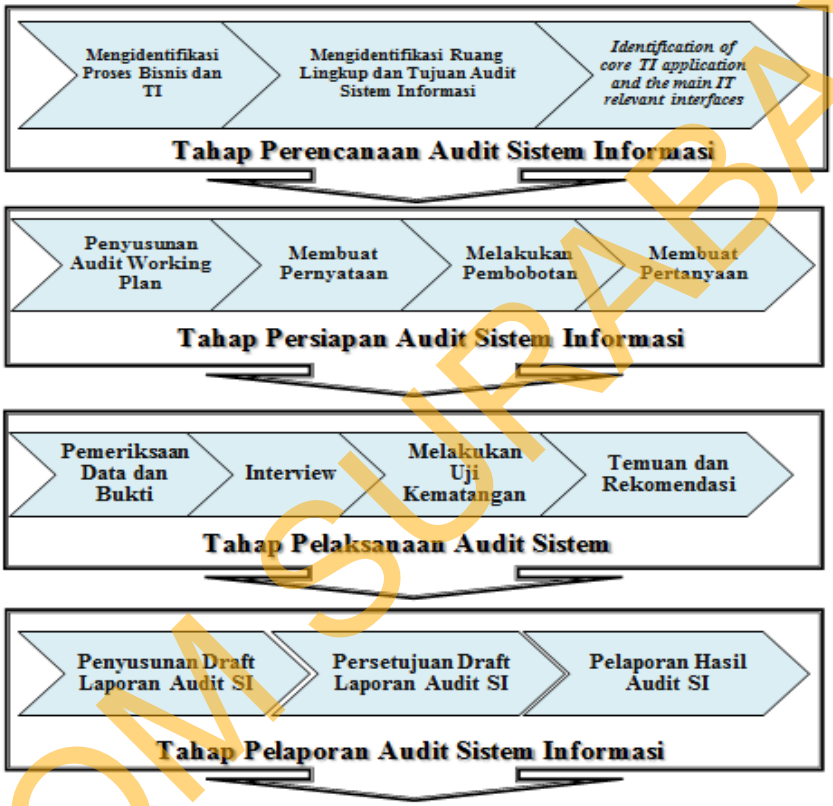
3. Tahap Pelaksanaan Audit Sistem Informasi

Pada tahap pelaksanaan, auditor melakukan pengumpulan dan evaluasi bukti dan data audit sistem informasi yang dilakukan, serta melakukan uji kepatutan (*complience test*), yakni dengan menyesuaikan keadaan ada dengan standar pengelolaan proses TI yang didefinisikan dalam kerangka kerja ISO 27002. Selanjutnya dilakukan penyusunan temuan serta rekomendasi guna diberikan kepada *auditee*.

4. Tahap Pelaporan Audit Sistem Informasi

Pada tahap pelaporan, auditor membuat *draft* pelaporan yang obyektif dan komperehensif yang nantinya ditunjukan ke *auditee*.

Tahapan-tahapan dalam audit sistem informasi merupakan langkah sekuensial. Setiap tahapan terdapat langkah-langkah yang harus dilakukan (Dhipiya, 2012). Tahapan-tahapan dalam audit sistem informasi dapat dilihat pada Gambar 2.4.



Gambar 2.4 Tahapan-Tahapan dalam Audit Sistem Informasi
(Sumber: Dhipiya, 2012)

2.4 Keamanan Informasi

Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimalisasi resiko bisnis (*reduce business risk*) dan memaksimalkan atau mempercepat pengembalian investasi dan

peluang bisnis (ISO/IEC 27001, 2005). Contoh keamanan informasi menurut Sarno dan Iffano (2009: 27) adalah sebagai berikut.

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 bahaya kebakaran, akses tanpa otorisasi, 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 beroperasi tanpa gangguan.
4. *Communications Security* adalah keamanan informasi bertujuan mengamankan media komunikasi, teknologi komunikasi, serta apa yang ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untu kemncapai tujuan organisasi.
5. *Network Security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringan, data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Aspek Keamanan Informasi meliputi ketiga hal, yaitu: *Confidentiality*, *Integrity*, dan *Availability* (CIA). Aspek tersebut dapat dilihat pada Gambar 2.5 di halaman 18, yang lebih lanjut akan dijelaskan sebagai berikut.

1. *Confidentiality*: Keamanan Informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses Informasi tertentu.
2. *Integrity*: Keamanan Informasi seharusnya menjamin kelengkapan Informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkannya berubah Informasi dari aslinya.
3. *Availability*: Keamanan Informasi seharusnya menjamin pengguna dapat mengakses Informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang bisa digunakan. Pengguna, dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses Informasi.

Gambar 2.5 Aspek Keamanan Informasi
(Sumber: Sarno dan Iffano, 2009: 37)

2.5 ISO/IEC 27002: 2005

International Standards Organization (ISO) mengelompokkan standar keamanan informasi yang umum dikenali secara internasional ke dalam struktur penomoran yang standar yakni ISO 17799. 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* dan *Technical Committee on Information Technology* (ISO/IEC 27002, 2005).

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 27001. 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*) yang dapat dilihat dalam Tabel 2.1. Sedangkan untuk detail struktur dokumen kontrol keamanan dari ISO/IEC 27001 dapat dilihat pada Lampiran 1.

Tabel 2.1 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

ISO 27002: 2005 tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhanya, dengan mempertimbangkan hasil kajian resiko yang telah dilakukanya (Direktorat Keamanan Informasi, 2011).

Pada Gambar 2.6 dapat dilihat bahwa *International Standards Organization* (ISO) mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, yaitu pada serial ISO 27000 (Sarno, 2009: 57).

<table>
<tr><td colspan="2">27000 Fundamental & Vocabulary</td></tr>
<tr><td rowspan="3">27005

RISK MANAGEMENT</td><td>27001: ISMS</td></tr>
<tr><td>27002: Code of Practice for ISMS</td></tr>
<tr><td>27003: Implementation Guidance</td></tr>
<tr><td rowspan="2">27004: Metrics & Measurement</td></tr>
<tr><td colspan="2">27006: Guidelines on ISMS Accreditation</td></tr>
<tr><td colspan="2">27007: Guidelines on ISMS Auditing</td></tr>
</table>

Gambar 2.6 ISO/IEC 27000 *Family*
(Sumber: Sarno dan Iffano, 2009: 56)

Standar tersebut memiliki fungsi dan peran masing-masing dan berkembang ke seri lain yang paparan lebih lanjutnya akan dijelaskan sebagai berikut.

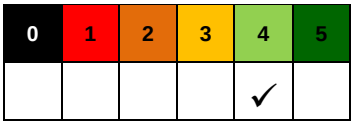
1. ISO/IEC 27000: merupakan dokumen yang berisikan definisi-definisi dalam bidang keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.
2. ISO/IEC 27001: berisi persyaratan standar yang harus dipenuhi untuk membangun SMKI.

3. ISO/IEC 27002: merupakan panduan praktis (*code of practice*) pelaksanaan, teknik, dan implementasi sistem manajemen keamanan informasi perusahaan berdasarkan ISO/IEC 27001.
4. ISO 27003: berisi panduan untuk perancangan dan penerapan SMKI agar meemenuhi persyaratan ISO 27001.
5. ISO 27004: berisi matriks dan metode pengukuran keberhasilan implementasi SMKI.
6. ISO 27005: dokumen panduan pelaksanaan manajemen resiko.
7. ISO 27006: dokumen panduan untuk sertifikasi SMKI perusahaan.
8. ISO 27007: dokumen panduan audit SMKI perusahaan.

2.6 Model Kedewasaan (*Maturity Model*)

IT Governance Institute (2007: 17) mendefinisikan model kedewasaan merupakan model yang digunakan untuk mengendalikan proses teknologi informasi yang terdiri dari pengembangan suatu metode penilaian sehingga suatu organisasi dapat mengukur dirinya sendiri.

Menurut DISC Infosec (2009) salah satu cara untuk mencapai kontrol keamanan informasi yang optimal adalah menilai keamanan informasi organisasi berdasarkan ISO 27002 dan memetakan setiap kontrol keamanan dengan *Capability Maturity Model Integration* (CMMI). CMMI memiliki lima tingkat tingkat kematangan proses yang dapat dilihat pada Gambar 2.7.



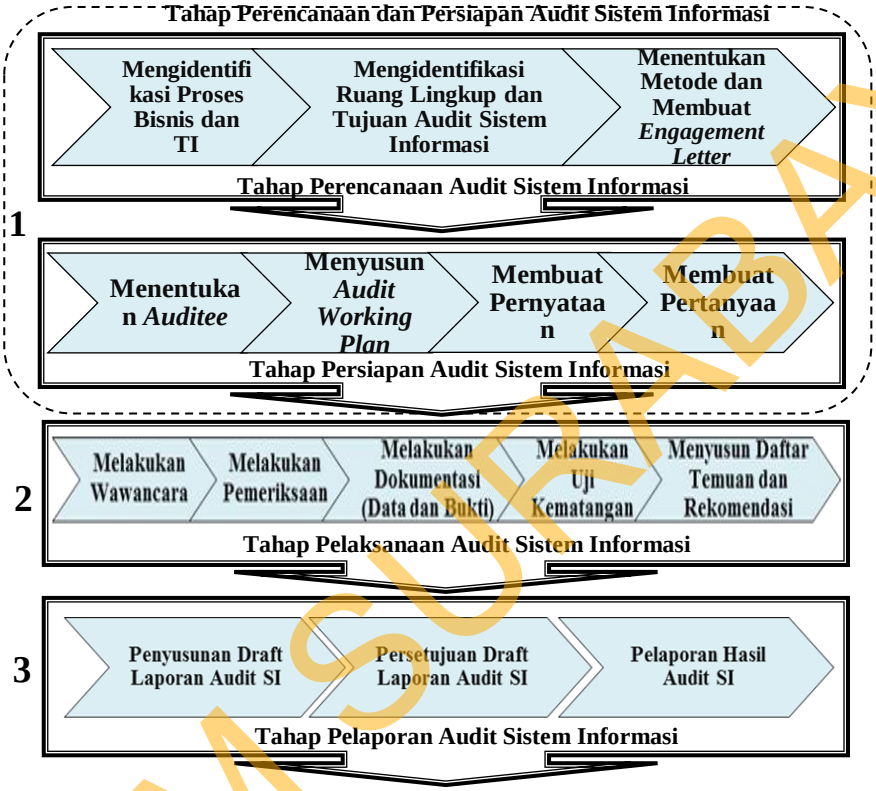
Gambar 2.7 Tingkat Kematangan CMMI
(Sumber: DISC Infosec, 2009)

Penilaian *maturity level* dilakukan menggunakan lima tingkatan proses rangkaian kesatuan kedewasaan berdasarkan metodologi CMMI. Pendekatan CMMI digunakan sebagai patokan untuk perbandingan dan berperan sebagai alat bantu untuk memahami tingkah laku, praktek, dan proses-proses dalam organisasi. Lima tingkatan kerangka kesatuan CMM adalah sebagai berikut.

a. Level 0 (*non-existent*): Tidak ada kontrol sama sekali.
b. Level 1 (*initial*): Pada level ini, organisasi memiliki pendekatan yang tidak konsisten, kontrol keamanan dilakukan secara informal. Informal berarti tidak ada dokumentasi, tidak ada standar.
c. Level 2 (*limited/repeatable*): Pada level ini, kontrol keamanan masih dalam pengembangan dan/atau ada dokumentasi terbatas untuk mendukung kebutuhan.
d. Level 3 (*defined*): Pada level ini, kontrol keamanan telah didokumentasikan rinci dan dikomunikasikan melalui pelatihan, tetapi tidak ada pengukuran kepatuhan.
e. Level 4 (*managed*): Pada level ini, terdapat pengukuran efektivitas kontrol keamanan, tetapi tidak ada bukti dari setiap ulasan kepatuhan dan/atau kontrol memerlukan perbaikan lebih lanjut untuk mencapai tingkat kepatuhan yang diperlukan.
f. Level 5 (*optimized*): Pada level ini, kontrol keamanan telah disempurnakan hingga sesuai dengan ISO 27002 berdasarkan pada kepemimpinan yang efektif, manajemen perubahan, perbaikan berkelanjutan, dan komunikasi internal.

2.7 Langkah-Langkah Kegiatan Audit Sistem Informasi

Langkah-langkah kegiatan audit yang akan dilakukan dapat dilihat pada Gambar 2.8.



Gambar 2.8 Langkah-Langkah Kegiatan Audit Sistem Informasi

1. Tahap Perencanaan dan Persiapan Audit Sistem Informasi

Tahap perencanaan dan persiapan ini dilakukan oleh auditor untuk mengetahui tentang *auditee* (*how your auditee*), mempelajari tentang proses bisnis perusahaan yang diaudit, merencanakan dan memantau pelaksanaan audit sistem informasi secara terperinci, menyusun audit *working plan*, serta mempersiapkan kertas kerja audit sistem informasi yang akan dipakai. Langkah-langkah yang terdapat di tahap perencanaan dan persiapan audit sistem informasi adalah sebagai berikut.

a. Mengidentifikasi proses bisnis dan TI

Dalam perencanaan proses audit, auditor harus melakukan pemahaman proses bisnis dan TI perusahaan yang diaudit (*auditee*). Pemahaman dilakukan dengan cara mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen tersebut bisa berupa profil perusahaan, rencana strategis, *standard operating procedure*, kebijakan, standar, prosedur, portofolio, arsitektur, infrastruktur, dan aplikasi sistem informasi. Auditor juga harus mengetahui apakah sebelumnya perusahaan telah dilaksanakan proses audit. Apabila pernah maka auditor juga mengetahui tentang laporan audit periode sebelumnya.

Pengetahuan tentang *auditee* dilakukan dengan cara melihat dokumen-dokumen yang terkait dengan proses audit dari media *online* bahkan auditor datang langsung ke perusahaan lalu melakukan wawancara awal kepada manajemen dan staf, serta melakukan observasi kegiatan operasional dan teknologi sistem informasi yang digunakan.

b. Mengidentifikasi ruang lingkup dan tujuan audit sistem informasi

Langkah selanjutnya yang dilakukan dalam audit sistem informasi adalah mengidentifikasi ruang lingkup. Ruang lingkup audit harus mengacu pada tujuan audit. Pada tahap ini auditor menentukan klausul, *objective control*, dan kontrol yang akan digunakan.

c. Menentukan metode dan membuat *engagement letter*

Pada tahap ini auditor merancang dan menentukan metode-medote yang akan digunakan pada pelaksanaan audit keamanan sistem informasi. Auditor menuangkan keseluruhan perencanaan audit ke dalam *engagement letter* beserta data-data apa saja yang dibutuhkan selama proses audit. Rencana audit harus

didiskusikan bersama pimpinan perusahaan sebelum disetujui oleh pimpinan perusahaan untuk memastikan kecukupan dukungan manajemen serta kesesuaian audit dengan kebutuhan manajemen (Hermawan, 2011).

d. Menentukan *auditee*

Auditee adalah entitas organisasi atau bagian/unit organisasi atau operasi/program termasuk kondisi tertentu yang diaudit. Penetapan *auditee* dilihat berdasarkan klausul yang telah ditetapkan. Selain itu, setelah dilakukan wawancara awal dapat ditentukan dan diketahui bagian mana saja yang menangani kontrol keamanan yang ada pada setiap klausul yang ditetapkan.

e. Menyusun jadwal audit (*Audit Working Plan*)

Audit *Working Plan* merupakan dokumen yang digunakan untuk merencanakan dan memantau pelaksanaan Audit TI secara terperinci. Dimulai dari proses awal hingga proses pelaporan audit.

f. Membuat pernyataan

Tahap selanjutnya dalam persiapan audit keamanan sistem informasi ini dilakukan dengan membuat pernyataan. Pernyataan dibuat berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah dipilih. Kontrol keamanan tersebut dapat dilihat pada panduan ISO 27002. Pada setiap kontrol keamanan dapat ditemukan pernyataan yang telah mendiskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut.

g. Membuat pertanyaan

Setelah dilakukan pembobotan pernyataan pada tiap proses TI, maka selanjutnya auditor membuat pertanyaan berdasarkan pernyataan tersebut.

Pertanyaan tersebut akan dijadikan acuan dalam melakukan wawancara kepada pihak yang telah ditentukan sebelumnya.

2. Tahap Pelaksanaan Audit Sistem Informasi

Pada tahap pelaksanaan, auditor melakukan pengumpulan dan evaluasi bukti dan data audit sistem informasi yang dilakukan, serta melakukan uji kepatutan (*complience test*), yakni dengan menyesuaikan keadaan yang ada dengan standar pengelolaan proses TI yang didefinisikan dalam kerangka kerja ISO. Selanjutnya dilakukan penyusunan temuan serta rekomendasi guna diberikan kepada *auditee*. Langkah-langkah yang terdapat di tahap pelaksanaan audit ini adalah sebagai berikut.

a. Melakukan wawancara

Wawancara dilakukan terhadap pihak-pihak yang terlibat dalam eksekusi. Proses TI yang dapat terbagi menjadi 4 kelompok, yaitu: pihak yang bertanggung jawab terhadap kesuksesan aktivitas (*responsible*), pihak yang bertanggung jawab (*accountable*), pihak yang mengerti aktivitas (*consulted*), dan pihak yang senantiasa diinformasikan perihal perkembangan aktivitas (*informed*). Wawancara juga dapat dilaksanakan berdasarkan struktur organisasi.

b. Melakukan pemeriksaan

Pemeriksaan terhadap data dan bukti dilakukan melalui 2 (dua) tahap test, yaitu: *compliance test* dan *substantive test*. *Compliance test* merupakan pengujian untuk mengetahui keberadaan/penerapan pengendalian dalam kegiatan operasional objek audit, sedangkan *substantive test* merupakan pengujian untuk memastikan kelengkapan, integritas, dan keakuratan (kebenaran dan kekonsistenan).

Pemeriksaan data dan bukti diambil saat pelaksanaan audit yang dilaksanakan berdasarkan pada program audit yang telah disiapkan pada tahap perencanaan dan persiapan audit dilakukan. Pembuatan kertas kerja dan pertanyaan-pertanyaan wawancara yang digunakan untuk mengumpulkan fakta tiap proses yang ada di sistem informasi saat ini, dimana pertanyaan yang diajukan dalam kertas kerja maupun wawancara dibuat dengan mengacu pada masing-masing kontrol proses sesuai pedoman dari ISO yang dikembangkan sesuai dengan objek yang akan diaudit.

c. Melakukan dokumentasi (data dan bukti)

Pada tahap ini auditor telah memperoleh data dan melakukan wawancara ataupun observasi yang akan membantu anggota tim ini untuk menganalisis data-data dan bukti-bukti yang ada. Selama melakukan audit, auditor harus dapat mendokumentasikan pekerjaan mereka sehingga kesimpulan dapat dibuktikan. Tujuan mendokumentasikan pekerjaan harus cukup detail sehingga cukup informasi bagi orang untuk dapat memahami apa yang telah dilakukan dan dapat mencapai kesimpulan yang sama seperti auditor. Dokumentasi dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Bukti-bukti tersebut dapat berupa foto, rekaman, data atau video.

d. Melakukan uji kematangan

Setelah dilakukan wawancara dan observasi pada tahap pengumpulan bukti, maka hasil audit yang diperoleh akan dianalisa dan dievaluasi. Analisa yang digunakan dalam audit keamanan sistem informasi kali ini adalah dengan menggunakan analisa tingkat kematangan. Uji kematangan dilakukan dengan menggunakan penilaian CMM *maturity level* dengan mengacu pada pernyataan

dari ISO 27002. Uji kematangan ini dilakukan untuk mengukur tingkat keamanan yang ada pada perusahaan.

e. Menyusun daftar temuan dan rekomendasi

Selama proses audit, auditor akan memeriksa banyak catatan, mempelajari banyak jenis informasi, melihat banyak laporan, mengobservasi prosedur kerja dan melakukan wawancara dengan berbagai pihak. Seluruh aktivitas tersebut menghasilkan bukti *(evidence)* yang berarti terkait dengan sistem yang berlangsung diperusahaan. Bukti tersebut akhirnya dikumpulkan dan dievaluasi untuk memungkinkan auditor membentuk opini mengenai kecukupan dan keefektifan kontrol internal sehingga dapat merekomendasikan tindakan perbaikan dan korektif (Sarno, 2009: 49).

3. Tahap Pelaporan Audit Sistem Informasi

Berdasarkan seluruh kertas kerja audit, temuan, dan tanggapan *auditee*, maka *audite* harus menyusun *draft* laporan audit keamanan sistem informasi sebagai pertanggungjawaban atas penugasan audit keamanan sistem informasi yang telah dilaksanakan. Laporan audit harus ditunjukan kepada pihak yang berhak saja karena laporan audit keamanan sistem informasi merupakan dokumen yang bersifat rahasia. Tahap pelaporan audit sistem informasi yang dilakukan dimulai dengan penyusunan *draft* laporan hasil audit, persetujuan *draft* laporan hasil audit, dan pelaporan hasil audit.