BAB II

LANDASAN TEORI

1. Definisi Sistem Informasi

Menurut Mulyadi dan Johny Setyawan (1999, halaman 34), sebuah sistem didefinisikan sebagai sebuah kelompok komponen-komponen yang saling berkaitan yang bekerja bersama untuk mencapai hasil yang diinginkan. Sistem informasi didefinisikan oleh Turban, Leidner, McLean dan Wetherbe (2007, halaman 16) sebagai pengumpulan, pemprosesan, analisis, dan penyebaran informasi untuk sebuah tujuan. Seperti pada sistem yang lain, sistem informasi memiliki *input* (data, instruksi) dan *output* (laporan, kalkulasi).

Ada bermacam-macam sistem informasi, salah satunya adalah *Management Information Systems* (MIS). Definisi dari MIS menurut Dittman, Bentley dan Whitten (2004, halaman 12) adalah sebuah sistem informasi yang mendukung pelaporan untuk manajemen yang berdasarkan proses transaksi dan operasi dari sebuah organisasi. Sehingga manajemen bergantung pada kemampuan MIS untuk menghasilkan sebuah laporan yang komprehensif, menyeluruh dan cepat.

2. Para Pemain dalam Sistem Informasi

Sistem informasi memiliki beberapa pemain di dalamnya, yaitu : *system owners* (pemilik sistem), *system users* (pengguna sistem), *system designers* (perancang sistem), *system builders* (pembangun sistem) *dan system analyst* (penganalisa sistem).

Pemilik sistem adalah orang yang bertanggung jawab dalam hal pendanaan, operasional, dan memelihara sistem informasi. Pemilik sistem ini biasanya adalah pimpinan perusahaan, atau pimpinan suatu departemen yang memiliki sebuah sistem informasi sendiri.

Pengguna sistem adalah siapa saja yang akan menggunakan sistem informasi secara terus menerus, yaitu orang yang memasukkan, memvalidasi, merespon, menyimpan, dan saling menukar data ataupun informasi. Pengguna sistem bisa dikelompokkan menjadi 2 yaitu eksternal dan internal. Yang termasuk internal adalah para penginput data, staf professional, pengawas, manajer tengah dan manajer eksekutif. Yang termasuk eksternal diantaranya adalah pelanggan, supplier, partner, dan karyawan yang bekerja di jalan ataupun di rumah.

Perancang sistem adalah seorang spesialis teknis yang menterjemahkan keperluan bisnis dari pengguna sistem dan juga hambatan-hambatan yang ada di dalamnya ke dalam sebuah solusi teknis. Orang ini yang merancang *database, input, output, screen, networks,* dan *software* yang akan memenuhi kebutuhan dari pengguna sistem. Mereka yang termasuk di dalamnya adalah: administrator *database*, arsitek jaringan, arsitek jaringan internet, ahli grafis, ahli keamanan IT, dan spesialis teknologi.

Pembangun sistem adalah seorang spesialis teknis yang membangun sistem informasi dan komponen-komponennya berdasarkan dari spesifikasi rancangan yang dibuat oleh perancang sistem. Mereka yang termasuk di dalamnya adalah pemprogram aplikasi, pemprogram sistem, pemprogram *database*, administrator jaringan, administrator keamanan, ahli internet dan pembuat piranti lunak.

Yang terakhir penganalisis sistem adalah seorang spesialis yang mempelajari permasalahan dan kebutuhan dari sebuah organisasi untuk menentukan bagaimana orang-orang, data, proses, dan teknologi informasi bisa memenuhi peningkatan kebutuhan dari bisnis. Seorang analis sistem harus mengerti aspek bisnis dan komputer. Mereka mempelajari permasalahan bisnis dan melihat kesempatan untuk kemudian mengubah kebutuhan bisnis akan informasi menjadi spesifikasi untuk sistem informasi yang akan diimplementasikan oleh berbagai spesialis teknis seperti pemprogram komputer. Komputer dan sistem informasi hanya

berharga bagi bisnis hanya jika mereka membantu memecahkan permasalahan atau mempengaruhi kinerja.

3. Komponen dalam Sistem Informasi

Komponen dalam sebuah sistem informasi ada banyak sekali, berikut ini definisi untuk beberapa komponen dalam sistem informasi yang akan banyak digunakan dalam karya akhir ini:

a. *Software*

Menurut Scott, George M dalam bukunya Prinsip-prinsip Sistem Informasi Manajeman (2000, halaman 216), sebuah *software* adalah program komputer yang fungsinya mengarahkan kegiatan pemrosesan dari komputer. Di dalam *software* berisi instruksi kepada komputer, atau pernyataan program yang secara tepat dinyatakan dan diorganisasikan sesuai dengan aturan tentang konstruksi program.

b. *Database*

Database didefinisikan sebagai sistem *file* komputer yang menggunakan cara pengorganisasian *file* tertentu, dimaksudkan untuk mempercepat pembaruan masing-masing *record*, serta pembaruan secara serempak atas *record* terkait, juga untuk mempermudah dan mempercepat akses terhadap seluruh *record* lewat program aplikasi, serta akses yang cepat terhadap data yang tersimpan yang harus digunakan secara bersama-sama untuk dibaca guna penyusunan laporan-laporan rutin ataupun khusus.

c. *Hardware*

Hardware adalah seperangkat alat seperti prosesor, monitor, *keyboard*, dan *printer*. Kesemuanya bekerja bersama-sama menerima data dan informasi, mengolahnya dan menampilkannya.

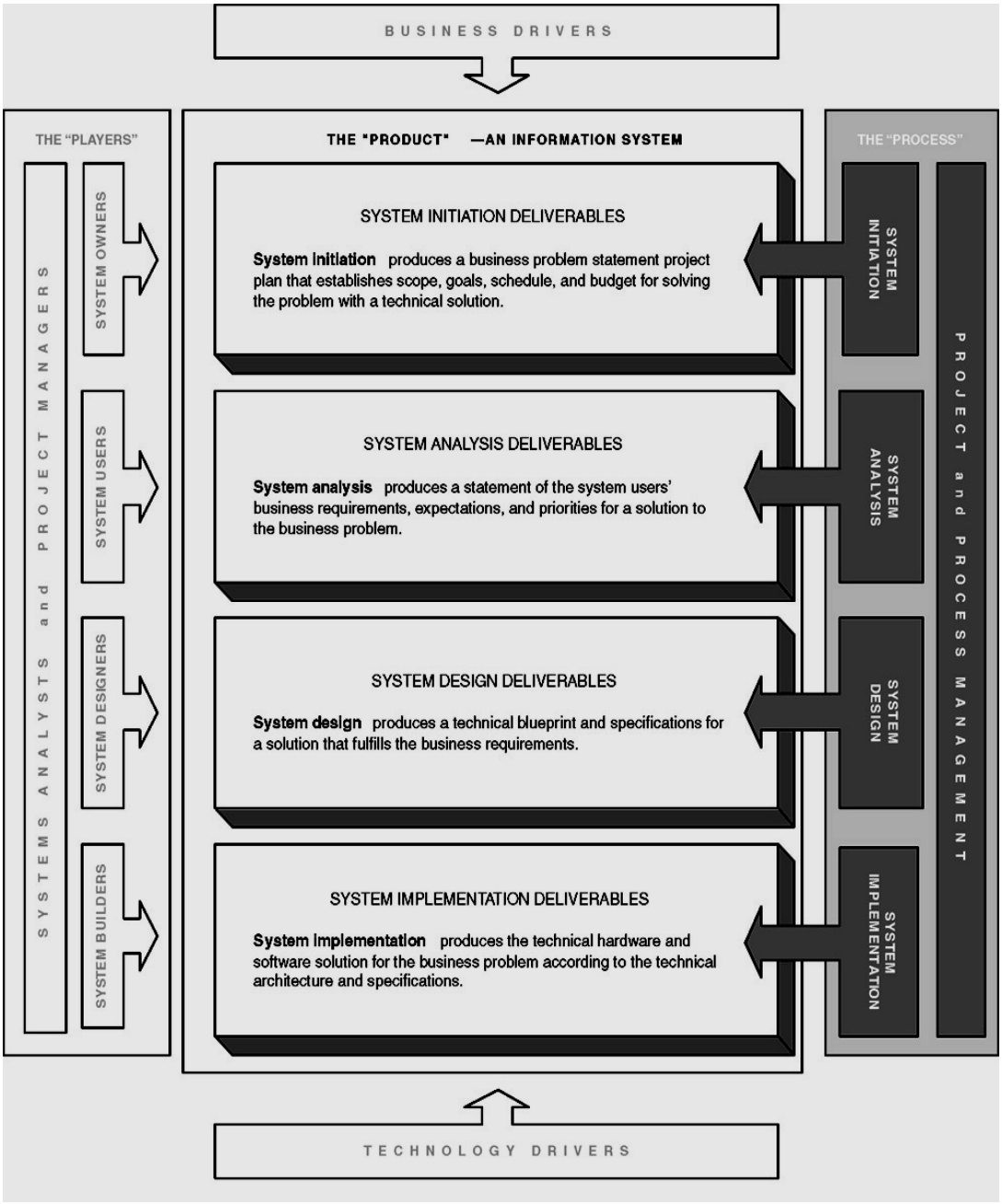
d. *Network*

Network adalah sebuah sistem yang saling berhubungan yang mengijinkan akses bersama dengan komputer yang lain. Saat ini sebuah *network* juga bisa saling berhubungan tanpa kabel.

4. Proses Membangun Sebuah Sistem

Tidak ada sebuah kerangka yang baku dalam membangun sebuah sistem. Pada umumnya proses membangun sebuah sistem bisa dikelompokkan menjadi empat tahapan seperti yang dikemukakan oleh Dittman, Bentley and Whitten (2004, hal 37) :

Gambar 2.1 Proses Pembangunan Sistem



Sumber : Dittman, Bentley and Whitten, hal 38.

a. Inisiasi Sistem

Sistem Inisiasi adalah dasar yang memulai perencanaan sebuah proyek yang mendefinisikan lingkup dari sebuah bisnis, tujuan, jadwal dan anggarannya. Di sini

langkah-langkah yang termasuk di dalamnya adalah pengidentifikasian permasalahan, dan juga perencanaan terhadap solusi dari permasalahan tersebut.

b. Analisis Sistem

Sistem Analisis mempelajari wilayah permasalahan bisnis untuk bisa merekomendasikan perbaikan atau menspesifikasi kebutuhan bisnis dan menentukan prioritas dari solusinya. Langkah-langkahnya yaitu: menganalisis dan mengerti duduk permasalahannya, kemudian mengidentifikasi kemungkinan kebutuhan atas solusinya atau pun mengidentifikasi ekspektasi dari permasalahan tersebut.

c. Perancangan Sistem

Sistem Perancangan mendefinisikan solusi dari sisi teknis atau *computer based* untuk kebutuhan bisnis yang diidentifikasikan di sebuah analisis sistem. Di sini perlu untuk mengidentifikasi solusi-solusi alternatif dan memilih solusi terbaiknya untuk kemudian merancang solusi yang sudah dipilih tersebut.

d. Implementasi Sistem

Sistem Implementasi adalah konstruksi, instalasi, tes dan penerapan dari sebuah sistem ke dalam sistem operasional sehari-hari. Di sini langkah-langkahnya adalah mengimplementasikan solusi yang sudah dipilih, dan mengevaluasi hasilnya. Jika permasalahannya tidak dipecahkan di sini, maka harus kembali ke langkah pertama atau sistem inisiasi.

e. *Support* Sistem dan Perbaikan yang Terus Menerus

Sistem Informasi yang diimplementasi jarang ada yang sempurna. Pengguna sistem biasanya akan menemukan kesalahan, dan sering kali disebabkan oleh proses perancangan dan implementasi yang kurang teliti melihat kesalahan tersebut. Perbaikan sistem informasi akan dilakukan terus menerus sampai pada suatu titik di mana perbaikan

yang dilakukan tidak dapat mengakomodir kebutuhan bisnis. Di saat seperti itu sebuah proyek baru akan dibuat.

5. Pengendalian Internal Teknologi Informasi

Suatu organisasi membutuhkan suatu pemahaman mendasar dari risiko dan hambatan yang dimiliki oleh TI di semua tingkat yang ada di dalam perusahaan untuk mencapai pengelolaan yang efektif dan pengendalian yang memadai. Hal ini juga berarti bahwa untuk mencapai hal tersebut, maka akan melibatkan berbagai pihak yang ada di dalam perusahaan.

Pengendalian internal merupakan kebijakan, prosedur, *practices* dan struktur organisasi yang diimplementasikan untuk mengurangi risiko. Pengendalian internal dibangun untuk memberikan suatu *assurance* yang *reasonable* kepada manajemen bahwa tujuan bisnis dapat dicapai dan risiko yang mungkin timbul akan dicegah, dideteksi dan dikoreksi.

Pengendalian internal teknologi informasi bertujuan untuk menjaga aset agar tetap *up to date* dan terhindar dari penyalahgunaan oleh pihak yang tidak diotorisasi; menjaga integritas lingkungan sistem operasi meliputi jaringan dan operasional, menjaga integritas dari lingkungan sistem aplikasi dengan cara otorisasi input, validasi input, keakuratan transaksi, keakuratan dan keamanan output yang dihasilkan, serta integritas, ketersediaan dan kerahasiaan database; menjamin autentifikasi user yang mengakses sumber daya TI, menjamin efisiensi dan efektifitas proses TI; menyesuaikan dengan kebutuhan user, kebijakan organisasi dan hukum yang berlaku; meningkatkan perlindungan terhadap data dan sistem dengan membangun *incident response plan*; menjamin integritas dan kehandalan sistem.

Menurut Ron Weber dalam bukunya *Information Systems Control and Audit* hal 49, terdapat lima komponen pengendalian internal, yaitu:

a. *Control environment*, meliputi filosofi manajemen dan cara operasional;
b. *Risk Assessment*, meliputi elemen yang mengidentifikasi dan menganalisis risiko yang dihadapi organisasi dan cara pengendalian risiko yang dilakukan organisasi;
c. *Control activities*, elemen yang dijalankan untuk: memastikan bahwa transaksi telah diotorisasi; telah ada pemisahan tugas; dokumen dan catatan penting dipelihara dengan baik; terdapat perlindungan aset; penilaian *performance*; *administrative controls*.
d. *Information and communication*
e. *Monitoring*

Pengendalian internal dapat bersifat pencegahan (*preventive*), pendeteksian (*detective*), dan *reactive*. Disebut *preventive* jika pengendalian yang ada akan mencegah terjadinya suatu hal yang buruk, contohnya user harus memasukkan *username* dan *password* jika ingin masuk ke suatu sistem. Secara teori, tindakan tersebut termasuk pengendalian yang bersifat mencegah agar sistem tidak diakses oleh pihak yang diotorisasi. Pengendalian hanya bersifat mendeteksi jika pengendalian tersebut mencatat terjadinya suatu yang buruk setelah hal tersebut terjadi. Pengendalian bersifat reaktif atau disebut juga *corrective controls* apabila pengendalian tersebut memberikan cara yang sistematik dalam mendeteksi terjadinya suatu hal yang buruk atau tidak diinginkan dan akan mengkoreksi hal yang buruk tersebut. Contohnya sistem memiliki antivirus yang akan mendeteksi jika ada hal buruk yang terjadi pada sistem.

Menurut *IT Governance Institute*, pengendalian internal di suatu organisasi mempengaruhi TI dalam 3 level yaitu:

a) Pada level eksekutif manajemen, manajemen harus menentukan tujuan bisnis, membuat suatu kebijakan, dan mengambil keputusan untuk mengembangkan dan

mengatur sumber daya yang terdapat di suatu organisasi dalam menjalankan strategi organisasi.

b) Pada level proses bisnis (*business process*), pengendalian diterapkan pada aktifitas bisnis. Kebanyakan proses bisnis telah terotomasi dan terintegrasi dengan sistem aplikasi TI, oleh karena itu diperlukan pengendalian yang baik. Pengendalian ini disebut sebagai pengendalian aplikasi (*application control*). Namun beberapa pengendalian dalam proses bisnis masih menggunakan prosedur manual seperti otorisasi transaksi, pemisahan tugas dan rekonsiliasi manual. Pengendalian dalam level proses bisnis merupakan kombinasi dari pengendalian manual dan otomasi dengan menggunakan pengendalian aplikasi.

c) Untuk mendukung proses bisnis, TI memberikan layanan ke berbagai proses bisnis. Pengembangan dan operasional proses TI diberikan bagi seluruh organisasi, melalui layanan seperti jaringan, database, sistem operasi dan penyimpanan (*storage*). Pengendalian yang digunakan untuk seluruh aktifitas layanan IT disebut pengendalian umum (*general control*). Kehandalan dari pengendalian umum ini dibutuhkan agar pengendalian aplikasi pun dapat dipercaya kehandalannya.

Pengendalian internal TI meliputi pengendalian umum dan pengendalian aplikasi. Pengendalian umum merupakan pengendalian yang “menempel” pada proses dan layanan TI, yang meliputi pengembangan sistem, perubahan manajemen, keamanan dan operasi komputer. Pengendalian umum diterapkan di semua area organisasi berupa kebijakan, standar dan prosedur yang mencakup organisasi dan manajemen yang bertanggung jawab dalam pengelolaan sumber daya teknologi informasi, pengembangan sistem dan aplikasi yang telah ada atau pembangunan sistem dan aplikasi yang baru, operasi komputer dan pemulihannya dari gangguan, serta akses terhadap perangkat keras, program, data dan sumber daya

teknologi informasi lainnya. Semua itu dilakukan agar tujuan organisasi dapat tercapai. Pengendalian umum ini meliputi pengendalian internal keuangan dalam menjaga aset dan kehandalan catatan laporan keuangan, pengendalian operasional untuk memastikan bahwa operasional yang dilakukan mendukung tujuan bisnis, pengendalian administratif yang mendukung pengendalian operasional, kebijakan dan prosedur keamanan organisasi untuk memastikan bahwa informasi dan teknologi digunakan dengan tepat, seluruh kebijakan yang dibuat untuk perancangan, penggunaan dokumen dengan tepat dan untuk memastikan ketepatan dalam pencatatan traksaksi; prosedur dan praktik untuk memastikan bahwa asset dan fasilitas yang ada diakses dan digunakan dengan tepat, kebijakan dalam hal *physical and logical security* untuk semua pusat data dan sumber daya TI.

Sedangkan, pengendalian aplikasi merupakan pengendalian yang "menempel" pada aplikasi yang mendukung proses bisnis. Pengendalian aplikasi merupakan pelindung atas integritas informasi dalam suatu organisasi agar dapat mengendalikan risiko yang timbul pada aplikasi seperti: *weak security, unauthorizes access to data, inaccurate information, Erroneous or falsified data input, Misused by authorized end users, incomplete processing, duplicate transactions, untimely processing, communications system failure*.

Pengendalian aplikasi merupakan metode untuk menjamin bahwa hanya data yang lengkap, akurat dan valid yang dimasukkan dan di-*update* dalam sistem komputer, proses komputer menjalankan tugas secara tepat, hasil proses sesuai dengan perkiraan dan integritas data terjaga.

Kelemahan mendasar pada area pengendalian umum akan mengakibatkan kelemahan pada aplikasi. Kelemahan pengendalian internal pada kedua area akan mengakibatkan sistem yang ada tidak dapat berjalan dengan baik.

6. Audit Teknologi Informasi

Menurut Komite Konsep Audit Dasar (*Committee on Basic Auditing Concepts*) yang dikutip dari buku *Auditing & Assurance Services: a Systematic Approach,* audit adalah suatu proses sistematis mendapatkan dan mengevaluasi bukti-bukti secara objektif sehubungan dengan asersi atas tindakan dan peristiwa ekonomi untuk memastikan tingkat kesesuaian antara asersi-asersi tersebut dan menetapkan kriteria serta mengkomunikasikan hasilnya kepada pihak-pihak yang berkepentingan.

Secara umum dikenal tiga jenis audit, yaitu audit keuangan, audit operasional dan audit TI. Audit TI adalah serangkaian pengujian yang dirancang untuk memastikan adanya pengendalian yang cukup atau memadai, untuk memberikan suatu tingkatan kepastian tertentu bagi pihak manajemen bahwa sistem komputer yang digunakan telah dapat melindungi aset milik organisasi; informasi dan data yang dimiliki dapat diandalkan; program secara akurat memproses transaksi-transaksi; karyawan telah memenuhi ketentuan kebijakan dan prosedur yang ditetapkan; dan terdapat sistem keuangan, *backup* yang memadai, dan prosedur lainnya yang cukup untuk mencegah kehilangan data akibat kerusakan atau modifikasi data yang tidak tepat, selain itu memastikan bahwa TI yang ada dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien. Audit TI relatif baru ditemukan dibanding audit keuangan, seiring dengan meningkatnya penggunan TI untuk mendukung aktifitas bisnis.

Ada beberapa aspek yang diperiksa pada audit TI: Audit secara keseluruhan menyangkut efektifitas, efisiensi, *availability system, reliability, confidentiality dan integrity, serta aspek security.* Selanjutnya adalah audit atas proses, modifikasi program, audit atas sumber data, dan data file.

Audit TI sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: *Traditional Audit*, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan *Behavioral Science*.

Di dalam audit TI, aspek yang harus diperhatikan adalah pengendalian internal, dimana pengendalian internal ini dapat dibedakan menjadi dua kategori, yaitu Pengendalian Aplikasi (*Application Control*) dan Pengendalian Umum (*General Control*). Pengendalian umum bertujuan untuk membuat kerangka pengendalian menyeluruh atas aktivitas TI dan untuk memberikan tingkat keyakinan yang memadai bahwa tujuan pengendalian internal secara keseluruhan dapat tercapai. Pengendalian umum lebih menjamin integritas data yang terdapat di dalam sistem komputer sekaligus meyakinkan integritas program atau aplikasi yang digunakan untuk melakukan pemrosesan data. Sedangkan pengendalian aplikasi bertujuan untuk mendeteksi dan mengkoreksi adanya kesalahan dan penyimpangan yang terjadi. Pengendalian aplikasi yang efektif akan menjamin kelengkapan dan keakurasian input, proses dan output. Dalam audit terhadap aplikasi, biasanya pemeriksaan atas pengendalian umum juga dilakukan mengingat pengendalian umum memiliki kontribusi terhadap efektifitas atas pengendalian-pengendalian aplikasi.

Sebelumnya audit TI dilakukan untuk mendukung audit laporan keuangan, namun saat ini tujuannya sudah lebih dari itu karena TI telah berkembang menjadi komponen penting dalam organisasi yang mampu mendukung tercapainya strategi dan tujuan organisasi. Dalam buku *Information Systems Control and Audit* oleh Weber dijelaskan bahwa kebutuhan akan audit berhubungan dengan hal-hal sebagai berikut:

a. Biaya yang ditanggung sehubungan dengan kehilangan data

   Data merupakan sumber daya yang sangat penting bagi organisasi. Data ini berkaitan dengan *image*, lingkungan, sejarah dan prospek organisasi di masa yang akan datang. Jika

data yang dimiliki organisasi akurat, maka kemampuan organisasi untuk beradaptasi akan meningkat dan mampu bertahan meskipun lingkungan organisasi berubah-ubah. Jika data tidak akurat atau banyak yang hilang, maka organisasi akan mengalami kerugian yang cukup subtansial. Kerugian tersebut bisa terjadi jika pengendalian terhadap komputer tidak memadai. Misalnya, manajemen organisasi tidak melakukan *back up* file komputer yang memadai, sehingga jika file hilang akibat program yang error, sabotase atau bencana alam, file tidak dapat di-*recovery*, akibatnya operasional organisasi akan terganggu;

b. Biaya sehubungan dengan pembuatan keputusan yang tidak tepat

   Keputusan yang memiliki kualitas yang baik sangat tergantung dari kualitas data dan kualitas *decision rules* yang ada dalam *computer based information systems*. Pentingnya keakuratan data pada sistem komputer tergantung dari tipe keputusan yang dibuat oleh orang yang memiliki kepentingan dalam organisasi tersebut. Contoh: jika manajer membuat keputusan dalam hal perencanaan strategi, mungkin ia akan mentoleransi beberapa data yang salah (*error*), namun jika ia harus membuat keputusan berkaitan dengan *management control* dan *operational control*, maka ia membutuhkan data yang sangat akurat.

c. Biaya sehubungan dengan perlakuan yang tidak wajar terhadap komputer

   Pendorong utama untuk melakukan audit TI adalah kejahatan terhadap sistem komputer seperti *hacking*, virus, akses fisik yang bersifat illegal, penyalahgunaan hak (*abuse of privileges*). Tindak kejahatan tersebut mengakibatkan kerusakan aset, pencurian aset, modifikasi aset, pelanggaran *privacy*, rusaknya operasional sistem yang akan mengganggu kelangsungan hidup organisasi. Kerugian yang diakibatkan oleh perlakukan tidak wajar terhadap komputer ini cukup tinggi. Saat ini tidak kejahatan semacam ini

semakin meningkat dan dengan maraknya internet yang tidak disertai dengan *security* yang baik mengakibatkan makin banyaknya virus yang menyerang komputer.

d. Nilai dari perangkat keras, perangkat lunak, dan para karyawan

Banyak organisasi telah menghabiskan jutaan dollar untuk berinvestasi dalam perangkat keras, meskipun perangkat keras tersebut telah diasuransikan, kehilangan perangkat keras baik yang disengaja maupun tidak, akan mengakibatkan kerugian yang cukup besar. Begitu juga apabila perangkat lunak mengalami kerusakan atau *corrupt* dan organisasi tidak dapat melakukan *recovery* dengan cepat, maka organisasi tidak dapat beroperasi. Selain data, perangkat keras dan perangkat lunak, karyawan merupakan sumber daya penting yang dimiliki organisasi, oleh karena itu karyawan harus diberikan pelatihan agar dapat menjadi *computer professional* yang baik dan terlatih.

e. Biaya tinggi dari kesalahan komputer (*computer error*)

Komputer saat ini memegang peranan penting di dalam masyarakat, akibatnya sistem komputer yang *error* akan memberikan kerugian yang besar. Contoh, ke-*error*-an sistem komputer yang digunakan untuk mengendalikan sistem penerbangan mengakibatkan kematian 257 orang, karena pesawat menabrak gunung di Antartika, sehingga perusahaan penerbangan tersebut harus membayar ganti rugi yang cukup tinggi akibat dari kecelakaan tersebut.

f. Pemeliharaan privasi

Saat ini, data-data yang terkait dengan individu telah terkomputerisasi, misalnya data tentang pajak, medis, pendidikan, tempat tinggal, pekerjaan, dan lain-lain. *Computer professional* harus memastikan bahwa data-data tersebut berkaitan dengan *privacy* seseorang sehingga tidak boleh disalahgunakan.

g. Evolusi yang terkontrol dari penggunaan komputer

Dari waktu ke waktu telah timbul perdebatan mengenai bagaimana sebaiknya teknologi komputer harus digunakan di masyarakat kita, agar jangan sampai teknologi komputer tersebut mengakibatkan hal yang buruk bagi masyarakat dan lingkungan sekitar. Contoh: beberapa ilmuwan menggunakan teknologi komputer untuk mendukung perkembangan senjata nuklir, tentunya hal ini merupakan hal yang berbahaya, sebab senjata nuklir dikhawatirkan akan mencelakakan manusia. Dari sini terlihat bahwa penggunaan komputer ada baik dan buruknya, oleh karena itu pemerintah, para profesional, organisasi atau individu itu sendiri harus senantiasa melakukan evaluasi dan monitoring agar jangan sampai teknologi komputer dipergunakan untuk hal yang tidak baik, membahayakan atau merugikan.

Dengan dilakukan audit TI diharapkan akan memberikan dampak positif bagi TI organisasi antara lain:

a. Memperbaiki sistem atau mekanisme perlindungan asset
b. Memperbaiki integritas data
c. Memperbaiki efektivitas sistem
d. Memperbaiki efisiensi sistem

7. **Tahapan Audit**

Dalam praktiknya, tahapan-tahapan dalam audit TI tidak berbeda dengan audit pada umumnya. Tahapan perencanaan, sebagai suatu pendahuluan, mutlak perlu dilakukan agar auditor mengenal benar objek yang akan diperiksa. Di samping, tentunya, auditor harus dapat memastikan bahwa *qualified resources* sudah dimiliki, dalam hal ini aspek SDM yang berpengalaman dan referensi praktik-praktik terbaik (*best practices*). Tahapan perencanaan ini akan menghasilkan suatu program audit yang didesain sedemikian rupa, sehingga

pelaksanaannya akan berjalan efektif dan efisien, dan dilakukan oleh orang-orang yang kompeten, serta dapat diselesaikan dalam waktu sesuai yang disepakati.

Dalam pelaksanaannya, auditor TI mengumpulkan bukti-bukti yang memadai melalui berbagai teknik termasuk survei, interview, observasi dan review dokumentasi (termasuk review *source-code* bila diperlukan). Bukti-bukti audit yang diambil oleh auditor biasanya mencakup pula bukti elektronis (data dalam bentuk file *softcopy*). Biasanya, auditor TI menerapkan teknik audit berbantuan komputer, disebut juga dengan CAAT (*Computer Assisted Auditing Technique*).

Sesuai dengan standar auditing ISACA (*Information Systems Audit and Control Association)*, selain melakukan pekerjaan lapangan, auditor juga harus menyusun laporan yang mencakup tujuan pemeriksaan, sifat dan kedalaman pemeriksaan yang dilakukan. Laporan ini juga harus menyebutkan organisasi yang diperiksa, pihak pengguna laporan yang dituju dan batasan-batasan distribusi laporan. Laporan juga harus memasukkan temuan, kesimpulan, rekomendasi sebagaimana layaknya laporan audit pada umumnya.

Menurut Ron Weber, langkah yang perlu dilakukan dalam melakukan audit adalah sebagai berikut:

a. *Planning the audit*

Pada tahapan ini *external auditor* akan melakukan hal-hal sebagai berikut :

a) Melakukan investigasi untuk memutuskan apakah akan melakukan *engagement* dengan seorang klien;
b) Melakukan pemilihan staf yang akan melakukan audit;
c) Membuat *engagement letter*;
d) Memperoleh informasi latar belakang klien;
e) Memahami kewajiban hukum dari klien;

f) Melakukan *analytical review procedure*, untuk memahami bisnis yang dimiliki oleh klien;

g) Menentukan area risiko.

Sedangkan pada tahapan ini *internal auditor* akan:

a) Memahami tujuan audit;

b) Memperoleh data-data organisasi;

c) Menugaskan staf untuk melakukan audit;

d) Mengidentifikasi area risiko.

Pada tahapan ini auditor harus memutuskan *preliminary materiality level*.

a. *Test of Control*

a) Melakukan penilaian terhadap risiko pengendalian;

b) Mengevaluasi pengendalian yang spesifik dan material;

c) Melakukan *management control*;

d) Melakukan *application control*

b. *Test of Transaction*

Langkah ini dilakukan untuk mengevaluasi apakah terdapat kesalahan dalam pemrosesan transaksi yang mengakibatkan salah saji material pada laporan keuangan, dengan melakukan *tracing journal entries*. Pada tahapan ini auditor dapat menggunakan *generalized audit software*.

c. *Test of Balances or Overall Results*

Langkah ini dilakukan untuk mendapatkan bukti (*evidence*) yang cukup agar dapat membuat *judgement* akhir terhadap kerugian atau salah saji akun yang terjadi akibat gagalnya fungsi sistem informasi dalam melindungi aset, menjaga integrasi data, dan memastikan bahwa sistem berjalan efektif dan efisien

d. *Completion of The Audit*

Pada tahapan ini dapat dilakukan beberapa pengujian tambahan untuk mengungkap bukti-bukti dan memberikan opini terhadap audit yang telah dilakukan.

Menurut Konrath (Konrath, 2002, 6), terdapat empat tahap utama dalam proses sistematik dari audit yang dapat dijabarkan sebagai berikut:

a. *Planning*

b. *Control Testing*, yaitu melakukan evaluasi atas pengendalian internal melalui:

   a) Mempelajari dan menguji pengendalian internal

   b) Menentukan sifat, waktu dan lingkup dari pengujian substantif yang akan dilaksanakan

c. *Substantive Testing*, yaitu melakukan pengujian transaksi dan saldo melalui:

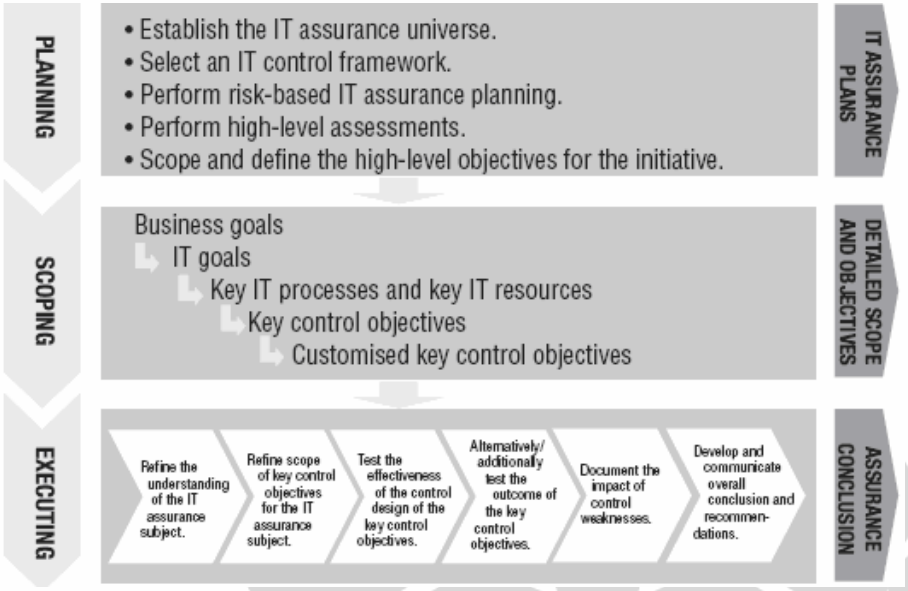
   a) Menguji transaksi dan saldo

   b) Mengevaluasi kewajaran dari komponen-komponen laporan keuangan

d. *Audit Report*

Sedangkan tahapan audit TI menurut COBIT dijabarkan dalam *IT Assurance Road Map, IT Assurance Guideline* (IT Governance Institute, 2007, 18). Di dalam *IT Assurance Road Map,* dijelaskan bahwa beberapa tahapan perlu dilakukan untuk memberikan suatu jaminan bahwa TI yang dimiliki telah memadai. Tahapan ini meliputi: *planning, scoping,* dan *executing*. Untuk tahap *executing* di *break-down* menjadi enam langkah sebagaimana ditunjukkan pada gambar berikut:

Gambar 2.2. Tahapan Audit COBIT



Sumber: IT Governance Institute, *IT Assurance Guide Using COBIT 4.1*, 2007

Tahapan *planning, scoping* dan *executing* dijabarkan dalam *IT Assurance Activities* sebagai berikut:

a. *Planning*

   a) Melakukan *quick risk assessment*;

   b) Menilai ancaman, serangan dan pengaruhnya bagi proses bisnis;

   c) Mendiagnosa *operational and project risk*;

   d) Merencanakan penilaian berdasarkan risiko;

   e) Mengidentifikasi proses-proses TI yang penting berdasarkan faktor pemicunya;

   f) Menilai *process maturity*;

b. *Scoping*

   a) *Scope* dan merencanakan *assurance*

   b) Memilih *control objectives* untuk proses-proses yang penting

   c) Menyesuaikan *control objectives*

c. *Executing*:

a) Memperbaiki pemahaman terhadap subjek dari *IT assurance* dengan cara:

- Mengidentifikasi/mengkonfirmasi proses-proses TI yang penting
- Melakukan *self assess process maturity*

b) Memperbaiki lingkup *key control objectives* tujuan pengendalian dengan cara:

- Meng-*update* pemilihan *control objective*
- Menyesuaikan *control objectives*
- Membangun audit program secara rinci

c) Menguji keefektifan *key control objectives* dengan cara:

- Menguji dan mengevaluasi pengendalian yang ada
- Mengupdate/menilai *process maturity*

d) Menguji hasil dari *key control objectives* dengan melakukan:

- *Self assess controls*
- Menguji dan mengevaluasi pengendalian yang ada

e) Mendokumentasikan pengaruh dari kelemahan pengendalian yang ada, dengan cara:

- Mendiagnosa *residual operational* dan atau risiko *project*;
- *Subtantiate risk.*

f) Membangun dan mengkomunikasikan seluruh kesimpulan dan rekomendasi dengan cara melaporkan seluruh kesimpulan atau hasil *assurance.*

Tahapan audit TI menggunakan COBIT sedikit berbeda dengan tahapan audit biasa. Audit TI menggunakan COBIT lebih seperti siklus pengembangan sistem (*Siklus Development Life Cycle*). Hal ini dapat dilihat dari keempat domainnya yaitu *Planning and Organize (PO), Acquire and Implement (AI), Delivery and Support (DS)* dan *Monitor and Evaluate (ME).*

Proses audit tidak akan berhenti sampai di *Monitor and Evaluate* saja, tapi akan berulang ke tahapan PO kembali, setelah hasil audit dari keempat domain tadi selesai dilakukan. Hal ini berbeda jika melakukan audit dengan metode biasa, yang akan berhenti jika proses audit telah selesai dilakukan, yaitu setelah dibuatnya laporan audit. Itu sebabnya, audit TI menggunakan COBIT sangat bermanfaat bagi auditor internal, dibanding auditor eksternal. Dengan melakukan audit menggunakan COBIT, manajemen TI akan mengetahui kondisi TI yang dimilikinya, dari nilai-nilai (*assurance*) yang dilakukan di setiap domain, serta hal-hal yang harus dilakukan untuk memperbaiki tata kelola TI di organisasinya. Sedangkan metode audit biasa lebih cocok digunakan oleh auditor eksternal, sebab prosesnya hanya sampai pada penyampaian laporan audit.

8. Metodologi COBIT (*Control Objectives for Information and related Technology)*

Metodologi COBIT adalah sebuah metodologi yang terbilang baru, karena baru dikeluarkan pada tahun 2007 oleh sebuah lembaga terkemuka di Amerika Serikat yaitu IT Governance Institute. Metodologi COBIT lebih menekankan kepada pembangunan sebuah IT yang berbasiskan *IT Governance*, yaitu sebuah sistem IT terpadu yang mendukung tercapainya strategi perusahaan dan tujuan perusahaan.

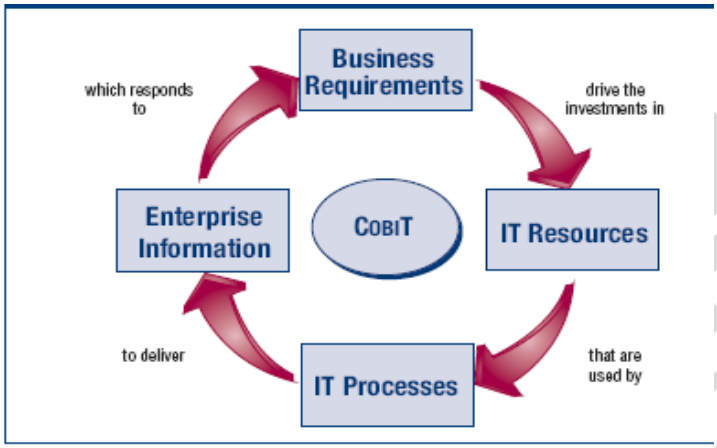
COBIT membantu mengoptimalkan TI dan memastikan TI yang digunakan oleh suatu organisasi telah memenuhi kebutuhan bisnis dari organisasi bersangkutan dan menjamin bahwa sumber daya TI digunakan dengan penuh tanggung jawab serta risiko yang ada mampu dikendalikan dengan baik.

COBIT dikembangkan oleh IT Governance Institute, yang merupakan bagian dari *Information Systems Audit and Control Association* (ISACA). COBIT memberikan arahan (*guidelines*) yang berorientasi pada bisnis, oleh karena itu *business process owners* dan

manajer, termasuk juga auditor dan user, diharapkan dapat memanfaatkan *guideline* ini dengan sebaik-baiknya.

Berikut ini adalah gambaran peranan konsep COBIT dalam bisnis :

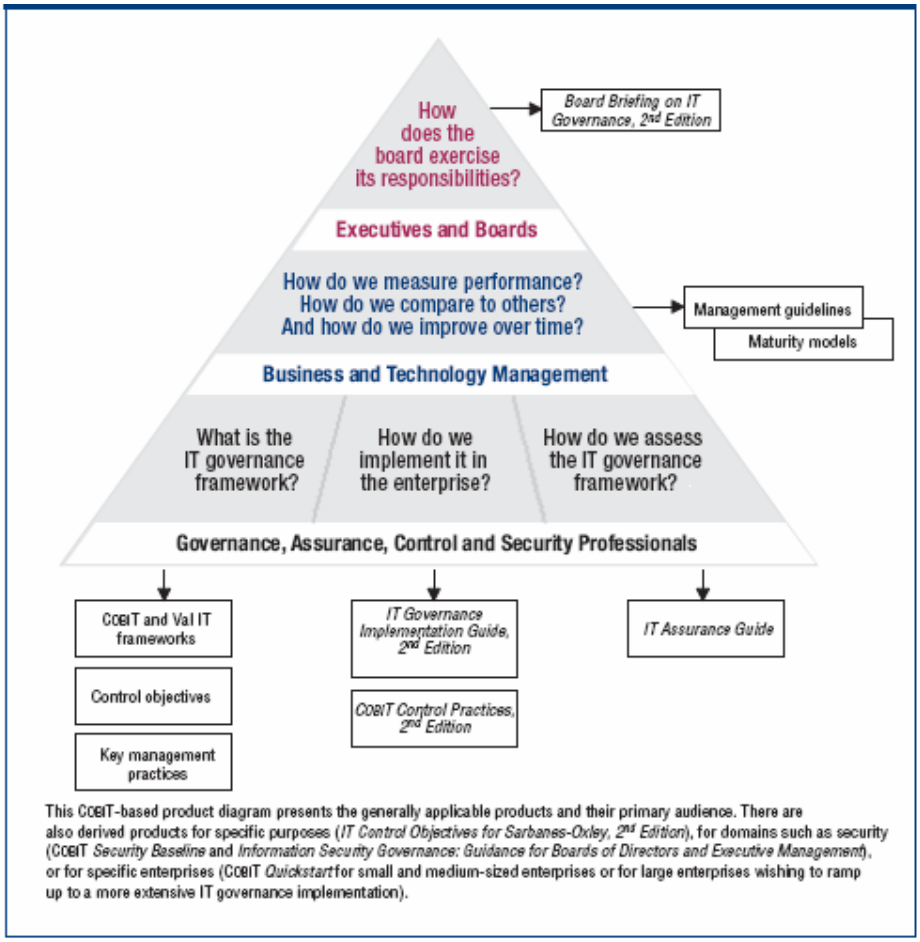
Gambar 2.3 Letak Konsep COBIT dalam Bisnis



Sumber : IT Governance Institute, hal 10.

Oleh karena itu dalam pembangunan IT, COBIT menyarankan agar IT harus sejalan dengan bisnis, harus memungkinkan bisnis memaksimalkan keuntungan, harus bertanggung jawab dalam penggunaan IT, dan risiko-risiko IT harus diatur secara benar. Salah satu keunggulan dari COBIT adalah COBIT mengukur hasil kinerjanya agar selaras dengan konsep *Balanced Scorecard* milik Robert Kaplan dan David Norton. Berikut ini adalah gambaran peran COBIT dalam suatu organisasi:

Gambar 2.4 Peran Konsep COBIT dalam Organisasi



Sumber : IT Governance Institute, hal 7.

COBIT memiliki empat *domain* seperti pada gambar 2.6 di bawah:

a. *Plan and Organise (PO)*

Domain ini yang menitikberatkan kepada proses perencanaan dan pengorganisasian penerapan TI, serta keselarasannya dengan tujuan organisasi/perusahaan secara umum. Dalam domain ini manajemen organisasi/perusahaan harus menjawab beberapa pertanyaan berikut:

a) Apakah TI dan strategi organisasi/perusahaan telah sejalan?
b) Apakah sumber daya yang ada telah digunakan secara optimal?
c) Apakah setiap orang di dalam organisasi/perusahaan telah memahami tujuan TI?
d) Apakah risiko TI telah dipahami dan dikendalikan dengan baik?

e) Apakah kualitas sistem TI telah sesuai dengan kebutuhan organisasi/perusahaan?

b. *Acquire and Implement (AI)*

Domain ini menitikberatkan kepada proses pemilihan dan penerapan teknologi yang akan diimplementasikan. Pada umumnya, pertanyaan yang harus dijawab pada domain ini adalah:

a) Apakah solusi yang diberikan telah sejalan dengan kebutuhan organisasi/perusahaan?
b) Apakah solusi dilakukan tepat waktu dan tidak melebihi biaya yang telah dianggarkan?
c) Apakah teknologi yang telah diimplementasikan tersebut akan berjalan dengan baik?
d) Apakah perubahan yang dibuat tidak akan mengacaukan proses organisasi yang sudah berjalan?

c. *Deliver and Support (DS)*

Domain ini menitikberatkan pada proses pelayanan yang diberikan oleh sistem TI yang diterapkan. Dalam domain ini manajemen organisasi/perusahaan harus menjawab beberapa pertanyaan berikut:

a) Apakah layanan TI yang diberikan telah sejalan dengan prioritas organisasi?
b) Apakah biaya TI telah optimal?
c) Apakah para pekerja dapat menggunakan sistem TI secara produktif dan aman?
d) Apakah kerahasiaan, integritas dan ketersediaan informasi telah terjamin?

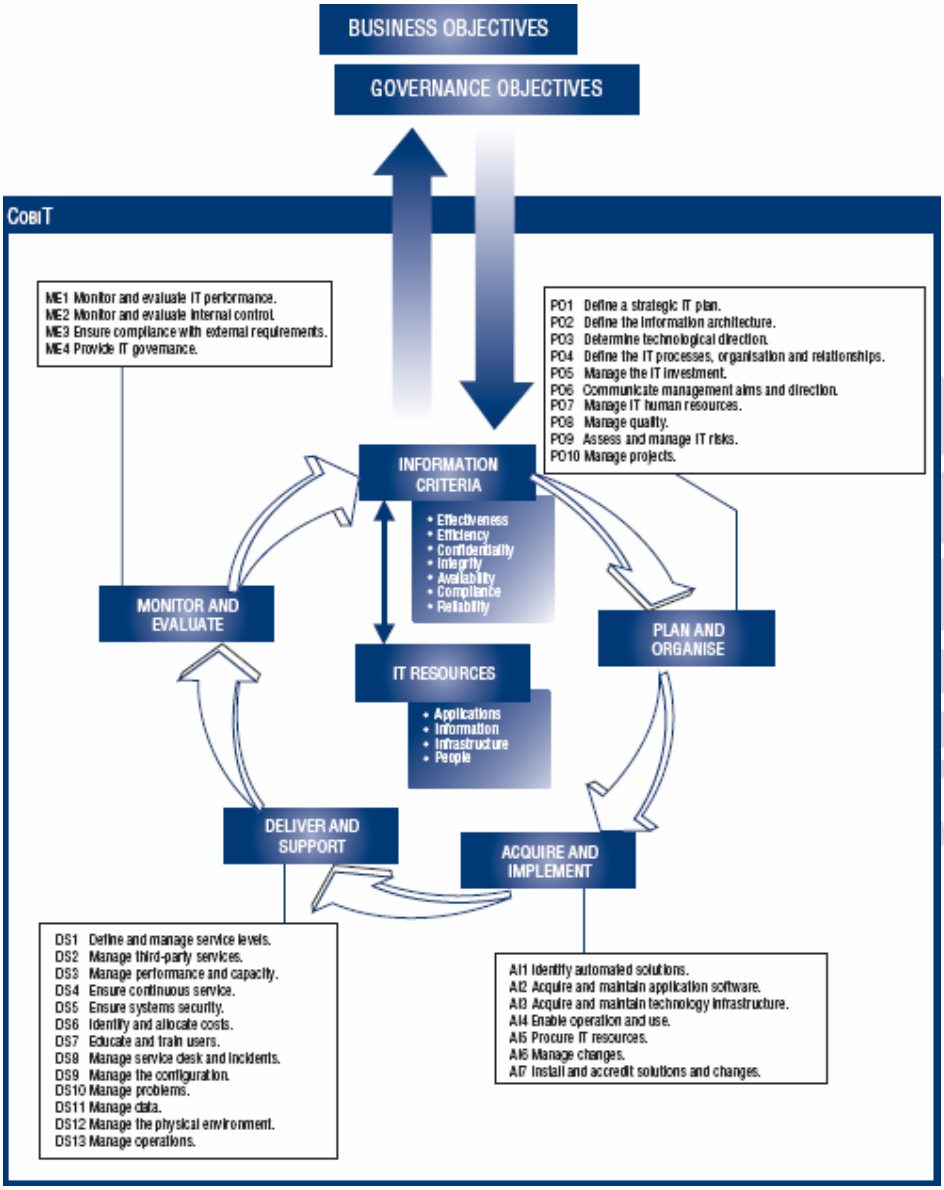
d. *Monitor and Evaluate (ME)*

Domain ini menitikberatkan pada proses pengawasan dan pengendalian kualitas layanan yang diberikan oleh sistem TI yang diterapkan. Seluruh proses IT harus dinilai kualitas dan kepatuhannya terhadap *control requirements*, secara reguler. Pertanyaan-pertanyaan yang biasanya muncul adalah:

a) Apakah performa TI dapat diukur untuk mendeteksi terjadinya suatu masalah sebelum semuanya terlambat?
b) Apakah manajemen telah yakin bahwa pengendalian internal telah berjalan efektif dan efisien?
c) Dapatkah performa TI memenuhi tujuan organisasi/perusahaan?

d) Apakah terdapat pengendalian yang memadai terhadap kerahasiaan, integritas dan ketersediaan informasi?

Gambar 2.5 *Domain* dalam COBIT



Sumber : IT Governance Institute, *IT Assurance Guide Using COBIT 4.1*, 2007

Keempat domain tersebut terbagi menjadi 34 proses yang meliputi: perencanaan (*plan*), pengembangan (*build*), pelaksanaan dan monitoring (*run and monitor*). Konsep arsitektur *enterprise*, seperti aplikasi, informasi, infrastruktur dan manusia, membantu untuk mengidentifikasi sumber daya yang penting bagi keberhasilan suatu proses. Agar informasi

yang ada dalam suatu organisasi mampu memberikan dukungan bagi organisasi dalam mencapai tujuannya, sumber daya TI yang ada harus dikelola dengan baik. Namun bagaimana organisasi yakin bahwa TI yang dimilikinya mampu memberikan informasi sesuai dengan kebutuhan organisasi? Apakah organisasi TI yang ada telah memiliki pengendalian yang baik? Bagaimana cara mengatasi risiko-risiko yang muncul? Bagaimana memastikan bahwa sumber daya TI yang dimiliki telah aman (*secure*)? Bagaimana organisasi yakin bahwa TI membantunya dalam mencapai tujuannya dan mendukung proses bisnis yang dimilikinya? Pertama, manajemen membutuhkan *control objective* yang mendefinisikan tujuan dari pengimplementasian kebijakan, rencana dan prosedur, serta struktur organisasi yang dirancang untuk memberikan kepastian bahwa tujuan bisnis telah dicapai dan kejadian yang tidak diinginkan dapat dicegah, dideteksi dan dikoreksi. Kedua, dalam lingkungan yang kompleks seperti sekarang ini, manajemen terus berusaha mendapatkan informasi yang akurat dan tepat waktu agar mampu menghasilkan keputusan yang tepat, bermanfaat, dan tidak berisiko. Untuk itu, bagaimana cara mengukurnya dan apa yang harus diukur? Organisasi membutuhkan suatu *objective measure* yang mengukur ada di "posisi" mana organisasi tersebut dan perbaikan apa yang dibutuhkan, dan organisasi tersebut harus membuat suatu *management tool kit* untuk memonitor perbaikan tersebut. Untuk memenuhi kebutuhan tersebut, dapat digunakan COBIT yang menyediakan:

a. *Maturity models* memungkinkan untuk dilakukan *benchmarking* dan menentukan upaya perbaikan yang diperlukan;
b. *Performance goals* dan *metrics* untuk proses-proses TI yang memberikan gambaran sejauh manakah setiap proses pengelolaan TI mampu memenuhi tujuan bisnis dan tujuan TI, dan digunakan untuk mengukur performa proses internal berdasarkan prinsip-prinsip *balanced scorecard*;

c. *Acitivity goals* yang memungkinkan tercapainya performa proses yang efektif.

Penilaian *process capability* berdasarkan COBIT *maturity model* merupakan bagian utama dari implementasi *IT governance*. COBIT memberikan dukungan bagi *IT governance* dengan memberikan kerangka kerja yang memastikan bahwa:

a. TI sejalan dengan bisnis/ tujuan organisasi
b. TI membuat organisasi mampu memaksimalkan manfaat (*benefit*) yang diperoleh
c. Sumber daya TI digunakan dengan tanggung jawab
d. Risiko-risiko TI dikendalikan dengan tepat

COBIT terfokus pada hal apa saja yang dibutuhkan untuk mendapatkan pengelolaan, manajemen dan pengendalian TI yang baik. Manfaat implementasi COBIT sebagai kerangka tata kelola TI yang baik adalah:

a. TI akan sejalan dengan proses dan strategi bisnis/organisasi;
b. Manajemen dapat memahami dan mengerti apa yang telah dilakukan TI;
c. *Ownership* dan tanggung jawab nampak jelas;
d. Dapat diterima oleh pihak ketiga dan para regulator;
e. Dapat dipahami oleh semua *stakeholder*, karena menggunakan "bahasa" yang sama yaitu COBIT;
f. Dipenuhinya syarat-syarat yang ditentukan oleh COSO dalam hal pengendalian TI.

Secara umum, sumber daya TI akan diatur oleh proses TI untuk mencapai tujuan TI yang merupakan respon terhadap kebutuhan bisnis/organisasi. COBIT akan sangat bermanfaat bagi:

a. *Executive management*, yang akan mendapatkan manfaat dari investasi TI yang dilakukannya, dengan COBIT *executive management* akan mampu menyeimbangkan risiko dan pengendalian TI yang harus dilakukan;

b. *Business management*, untuk mendapatkan jaminan dan pengendalian TI yang diberikan oleh internal organisasi atau pihak ketiga;

c. *IT management*, untuk memberikan layanan TI yang dibutuhkan dalam suatu proses bisnis demi mendukung tercapainya strategi organisasi.

d. Auditor, untuk mendukung opininya dan atau memberikan saran bagi manajemen dalam melakukan pengendalian internal.

Kontribusi yang diberikan COBIT bagi suatu organisasi adalah:

a. Menghubungkan antara kepentingan bisnis dan tujuan TI

b. Mengelola aktifitas TI dengan baik sehingga menjadi *generally accepted process model*

c. Mengidentifikasi sumber daya TI yang perlu ditingkatkan

d. Menentukan *management control objectives* yang harus dipertimbangkan

e. Terdapat *tools* yang dapat digunakan oleh manajemen yaitu:

    a) *Goals dan metrics* untuk mengukur peformance TI

    b) *Maturity model* untuk mengukur *process capability*

    c) *Responsible, Accountable, Consulted and Informed (RACI) charts* untuk menjelaskan peran dan tanggung jawab masing-masing pihak.

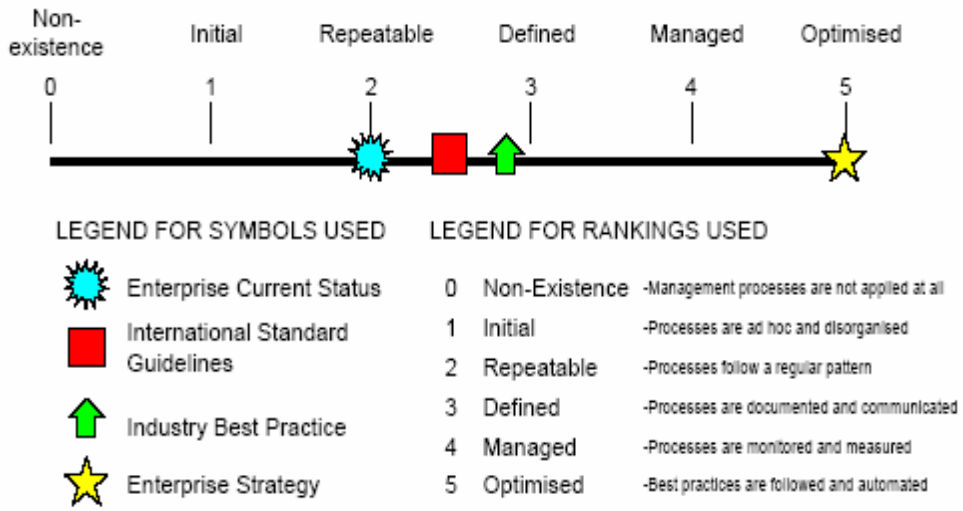
COBIT memberikan gambaran yang jelas mengenai hubungan antara kebutuhan dalam tata kelola TI, proses TI dan pengendalian TI. Mengelola dan mengendalikan informasi serta membantu agar TI sejalan dengan kebutuhan bisnis adalah inti dari kerangka COBIT. Manajemen harus terus melakukan analisis untuk melihat pengendalian apa yang diperlukan untuk memastikan bahwa risiko dapat dikendalikan.

9. Maturity Model

Suatu organisasi harus memahami sistem TI yang dimilikinya agar dapat menentukan pengendalian dan perbaikan yang tepat bagi sistem TI tersebut. Untuk menentukan berada di level mana sistem TI yang dimilikinya, maka organisasi harus melakukan pengukuran untuk menentukan perbaikan apa yang diperlukan dan harus mengimplementasikan *tools* untuk memonitor perbaikan tersebut.

Maturity modelling bagi manajemen dan pengendalian terhadap proses TI, didasarkan pada metode yang digunakan untuk mengevaluasi organisasi. Nilai dalam *maturity model* ini memiliki *range* dari level *non-existent* (0) sampai dengan *optimised* (5), hal ini ditunjukkan pada gambar 2.6 di bawah ini.

Gambar 2.6 Rentang nilai *maturity model*



Sumber : IT Governance Institute, *IT Assurance Guide Using COBIT 4.1*, 2007

Dengan menggunakan *maturity model* maka manajemen dapat melakukan identifikasi terhadap:

a. *Performance* sebenarnya dari organisasi

b. Kondisi dan status industri saat ini

c. Target organisasi dalam melakukan perbaikan

d. Tingkat pertumbuhan yang diinginkan

Penentuan *range* nilai dari 0 (*Non*-existent) sampai dengan 5 (*Optimised*) dijabarkan dalam *Generic maturity model* sebagai berikut:

a. 0 (*Non-Existent*), dimana suatu organisasi sama sekali tidak memiliki suatu proses, dan bahkan belum mengenal isu yang perlu dipertimbangkan.

b. 1 (*Initial*), dimana suatu organisasi telah mengenali adanya isu tertentu, namun belum terdapat proses yang terstandarisasi, tetapi hanya memiliki pendekatan informal yang cenderung diterapkan secara individu atau kasus per kasus. Secara umum, pendekatan yang digunakan masih belum terorganisir secara baik.

c. 2 (*Repeatable but Intuitive*), proses yang ada telah berkembang ke dalam tahapan dimana beberapa prosedur yang sama digunakan dan diikuti oleh orang-orang yang berbeda yang menjalankan tugas yang sama. Belum ada pelatihan atau komunikasi yang formal atas prosedur-prosedur standar, tanggung jawab diemban oleh masing-masing individu. Terdapat tingkat ketergantungan yang tinggi terhadap pengetahuan dari masing-masing individu, sehingga error/kesalahan sering terjadi

d. 3 (*Defined*), dimana prosedur telah distandarisasi, didokumentasikan, dan dikomunikasikan melalui pelatihan. Namun, proses-proses tadi masih diberikan atau ditinggalkan kepada individu untuk mengikutinya, dan penyimpangan yang terjadi dari hal tersebut belum bisa dideteksi. Prosedur yang ada masih relatif sederhana dan belum memadai.

e. 4 (*Managed and Measurable*), dimana organisasi telah melakukan monitoring dan mengukur kepatuhan dalam menjalankan prosedur yang telah ditetapkan, serta mengambil tindakan yang perlu pada saat suatu proses berjalan tidak semestinya. Setiap

proses yang berjalan berada dalam perbaikan yang berkesinambungan. Berbagai alat bantu dan otomatisasi sudah mulai digunakan meskipun masih terbatas dan masih terpisah-pisah.

f. 5 (*Optimised*), dimana proses telah diperbaiki sampai ke tingkat yang terbaik, yang merupakan hasil dari perbaikan secara terus menerus (*continues* improvement). TI telah digunakan secara terintegrasi untuk melancarkan *workflow*, memberikan alat bantu untuk memperbaiki kualitas dan efektivitas, serta menjadikan organisasi fleksibel dan cepat dalam melakukan perubahan.

Setelah mengetahui kondisi organisasi, *Maturity Model* akan memberikan peluang kepada organisasi untuk melakukan perbandingan terhadap tuntutan standar internasional, terhadap praktik terbaik di lingkungan organisasi, dan terhadap strategi organisasi. Sehingga akan membantu manajemen organisasi untuk menentukan kekurangan manajemen TI, dan membantu mereka untuk menentukan sasaran berdasarkan perbandingan sebelumnya. Secara khusus, tingkat kedewasaan pengendalian akan tergantung pada ketergantungan organisasi terhadap TI, kecanggihan teknologi dan yang terpenting adalah nilai dari informasinya.

Maturity model merupakan cara seberapa baik proses manajemen yang ada, contohnya seberapa baik kemampuan manajemen tersebut. Seberapa baik kemampuan proses manajemen tersebut tergantung dari tujuan TI dan dukungan TI tersebut terhadap jalannya proses manajemen.

Skala *maturity model* akan membantu professional untuk menjelaskan kekurangan manajemen proses TI kepada pihak manajemen dan membantu menentukan target yang ingin dicapai. Level *maturity* akan dipengaruhi oleh tujuan perusahaan, lingkungan operasional dan praktik industri. Level *management maturity* akan tergantung dari ketergantungan organisasi terhadap TI, kepuasan teknologi dan yang paling penting adalah nilai dari informasi.

Dengan menggunakan *maturity model*, manajemen dapat melakukan identifikasi terhadap:

a. Performa organisasi/perusahaan saat ini;
b. Status organisasi/perusahaan di suatu lingkungan/industri dibandingkan dengan organisasi/perusahaan lain yang berada di lingkungan/industri yang sama;
c. Target perbaikan yang ingin dilakukan organisasi/perusahaan
d. Tingkat pertumbuhan yang diinginkan oleh organisasi/perusahaan