# BAB II

# LANDASAN TEORI

## 2.1. Pengertian Audit

Audit merupakan suatu proses pengumpulan data, penilaian ataupun pengevaluasian yang dilakukan untuk menilai sesuatu apakah telah sesuai dengan kriteria yang mendasarinya. Secara umum, audit adalah proses pengevaluasian atas suatu kegiatan untuk menilai apakah kegiatan tersebut sudah sesuai dengan standarnya. Pada dasarnya setiap audit bertujuan untuk menilai apakah pelaksanaan kegiatan sudah selaras dengan yang digariskan.

Audit adalah Suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara obyektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan.[4] Berdasarkan definisi *auditing* secara umum memiliki unsur penting yaitu :

1. Proses yang Sitematis; Yaitu mengandung makna sebagai rangkaian langkah atau prosedur yang logis, terencana, dan terorganisasi.
2. Memperoleh dan Menilai Bukti Secara Obyektif; Yaitu mengandung arti bahwa auditor memeriksa dasar-dasar yang disepakati untuk membuat aserasi atau pernyataan oleh manajemen dan melakukan penilaian tanpa sikap memihak.

3. Tindakan-tindakan dan Kejadian-kejadian Ekonomi; Yaitu pernyataan tentang kejadian ekonomi yang merupakan informasi hasil proses akuntansi yang dibuat oleh individu atau suatu organisasi.

4. Mengkomunikasikan Hasilnya kepada Pihak-pihak yang Berkepentingan; Yaitu kegiatan terakhir dari suatu *auditing* atau peng-auditan adalah menyampaikan temuan-temuan dan hasilnya kepada pengambil keputusan.

5. Tingkat Kesesuaian Kriteria yang Telah Ditetapkan; Yaitu secara spesifik memberikan alasan mengapa auditor tertarik pada pernyataan bukti-bukti pendukungnya.

*Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria. Auditing should be done by a competent independent person*". *Auditing* adalah proses pengumpulan dan evaluasi bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi untuk menentukan dan melaporkan kesesuaian informasi dengan yang telah ditetapkan. *Auditing* seharusnya dilakukan oleh orang yang kompeten dan independen.[5] Definisi *auditing* meliputi beberapa konsep penting, [5, p. 11]

**a**) Informasi dan kriteria yang ditetapkan *(Information and established criteria).*

b) Mengumpulkan & evaluasi bukti *(Accumulating and evaluating evidence).*

**c**.) Orang kompeten dan tidak memihak *(Competent, independent person).*

**d.)** Pelaporan *(Reporting*).

### 2.1.1. Tipe-tipe Audit

Audit pada umumnya dibagi menjadi tiga golongan, yaitu audit laporan keuangan, audit kepatuhan, dan audit operasional.

1. Audit laporan keuangan (*financial statement audit*). Audit laporan keuangan *(audit of financial statement).* Audit laporan keuangan lebih mengarah pada laporan keuangan secara keseluruhan dan kualitas informasi yang dihasilkan. Bertujuan menentukan apakah laporan keuangan secara keseluruhan yang merupakan informasi terukur yang diverifikasi dan telah disajikan sesuai dengan kriteria tertentu.
2. Audit kepatuhan *(compliance audit).* Audit ketaatan yaitu auditor menentukan apakah perusahaan sudah berjalan sesuai dengan peraturan yang ada. Bertujuan mempertimbangkan apakah *auditee* (klien) telah mengikuti prosedur atau aturan tertentu yang telah ditetapkan pihak yang memiliki otoritas lebih tinggi.
3. Audit operasional *(operational audit).* Audit operasional yaitu merupakan penelaahan atas bagian manapun dari prosedur dan metode operasi suatu organisasi untuk menilai efisiensi dan efektifitasnya. Umumnya pada saat selesainya audit operasional, auditor akan memberikan sejumlah saran kepada manajemen untuk memperbaiki jalannya operasi perusahaan. Tujuan audit operasional adalah untuk :

a. Menilai kinerja, kinerja dibandingkan dengan kebijakan-kebijakan, standar-standar, dan sasaran-sasaran yang ditetapkan oleh manajemen
b. Mengidentifikasikan peluang, dan

c. Memberikan rekomendasi untuk perbaikan atau tindakan lebih lanjut. Pihak-pihak yang mungkin meminta dilakukannya audit operasional adalah manajemen dan pihak ketiga. Hasil audit operasional diserahkan kepada pihak yang meminta dilaksanakannya audit tersebut.

### 2.1.2. Jenis-jenis Auditor

Berdasarkan kelompok atau pelaksana audit, [4] audit dapat dibagi menjadi :

1. *Auditor Eksternal.* Audit eksternal merupakan pihak luar yang bukan merupakan karyawan perusahaan, berkedudukan independen dan tidak memihak baik terhadap *audite*-nya maupun terhadap pihak-pihak yang berkepentingan dengan *audite*-nya (pengguna laporan keuangan). Auditor eksternal dapat melakukan setiap jenis audit.

2. *Auditor Internal.* Auditor internal adalah pegawai dari perusahaan yang di-audit, auditor ini melibatkan diri dalam suatu kegiatan penilaian independen dalam lingkungan perusahaan sebagai suatu bentuk jasa bagi perusahaaan.. **Fungsi dasar dari Internal Audit** adalah suatu penilaian, yang dilakukan oleh pegawai perusahaan yang terlatih mengenai ketelitian, dapat dipercayainya, efisiensi, dan kegunaan catatan-catatan (akutansi) perusahaan, serta pengendalian intern yang terdapat dalam perusahaan. Tujuannya adalah untuk membantu pimpinan perusahaan (manajemen) dalam melaksanakan tanggung jawabnya dengan memberikan analisa, penilaian, saran, dan komentar mengenai kegiatan yang di-audit. Dari kegiatan-kegiatan yang dilakukannya tersebut dapat disimpulkan bahwa internal auditor antara lain memiliki peranan dalam Pencegahan Kecurangan

*(Fraud Prevention)*, Pendeteksian Kecurangan *(Fraud Detection)*, dan Penginvestigasian Kecurangan *(Fraud Investigation).*

3. *Auditor Pajak.* Auditor pajak bertugas memeriksa ketaatan wajib pajak yang diaudit terhadap Undang-undang yang berlaku.

4. *Auditor Pemerintan.* Tugas auditor pemerintah adalah memeriksa kewajaran informasi keuangan yang disusun oleh instansi pemerintahan.Disamping itu, audit juga dilakukan untuk menilai efisiensi dan efektifitas serta ekonomisasi operasi program dan penggunaan barang milik pemerintah.

## 2.2. Konsep Dasar Sistem Informasi

### 2.2.1. Definisi Sistem

Menurut *O'Brien James A*, sistem merupakan sekumpulan komponen komponen yang saling berhubungan dan bekerja sama untuk mencapai tujuan bersama, dengan menerima masukan dan menghasilkan pengeluaran melalui proses transformasi yang terorganisir.

Pendekatan sistem yang menekankan pada prosedur mendefinisikan sistem sebagai berikut ini. ”Suatu sistem adalah suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran yang tertentu”.[3] Dari definisi-definisi tersebut dapat ditarik kesimpulan bahwa sistem adalah kumpulan dari komponen-komponen atau subsistem-subsistem yang saling berinteraksi dan berhubungan membentuk satu kesatuan untuk mencapai tujuan atau sasaran sistem tersebut.

### 2.2.2. Definisi Informasi

informasi adalah ”data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya”.[3] Data merupakan kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata. Data merupakan bentuk mentah yang perlu diolah lebih lanjut melalui suatu model untuk dihasilkan informasi. Kejadian-kejadian *(event)* adalah sesuatu yang terjadi pada saat yang tertentu. Kesatuan *(fact dan entity)* adalah berupa suatu obyek nyata seperti tempat, benda dan orang yang betul-betul ada dan terjadi.

Suatu informasi dapat mempunyai nilai. Nilai dari informasi dapat ditentukan dengan dua hal, yaitu manfaat dan biaya mendapatkannya. Suatu informasi dikatakan bernilai bila manfaatnya lebih efektif dibandingkan dengan biaya mendapatkannya. Kualitas dari suatu informasi *(quality of information)* tergantung dari tiga hal, yaitu informasi harus akurat *(accurate)*, tepat pada waktunya *(timeliness)*, dan relevan *(relevance)*.[3]

1. Akurat, berarti informasi harus bebas dari kesalahan-kesalahan dan tidak bias atau menyesatkan.
2. Tepat pada waktunya, berarti informasi yang datang pada penerima tidak boleh terlambat.
3. Relevan, berarti informasi tersebut mempunyai manfaat untuk pemakaiannya.

### 2.2.3. Pengertian Sistem Informasi

Sistem informasi didefenisikan oleh Robert A. Leitch dan K. Roscoe Davis sebagai berikut ”Sistem informasi adalah suatu sistem di dalam suatu organisasi

yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan". John Burch dan Gary Grudnitski mengemukakan bahwa sistem informasi terdiri dari komponen-komponen yang disebutnya dengan istilah blok bangunan *(building block),* yaitu terdiri dari 6 blok yang masing-masing saling berinteraksi dan membentuk satu kesatuan untuk mencapai sasarannya.[3] Keenam blok tersebut adalah :

a. **Blok Masukan**. Input mewakili data yang masuk ke dalam sistem informasi. Input disini termasuk metode-metode dan media untuk menangkap data yang akan dimasukkan, yang dapat berupa dokumen-dokumen dasar.

b. **Blok Model.** Blok ini terdiri dari kombinasi prosedur, logika dan model matematik yang akan memanipulasi data input dan data yang tersimpan di basis data dengan cara yang sudah tertentu untuk menghasilkan keluaran yang diinginkan.

c. **Blok Keluaran**. Produk dari sistem informasi adalah keluaran yang merupakan informasi yang berkualitas dan dokumentasi yang berguna untuk semua tingkatan manajemen serta semua pemakai sistem.

d. **Blok Teknologi.** Teknologi digunakan untuk menerima input, menjalankan model, menyimpan dan mengakses data, menghasilkan dan mengirimkan keluaran dan membantu pengendalian dari sistem secara keseluruhan..

Teknologi terdiri dari 3 bagian utama, yaitu teknisi (*humanware* atau *brainware*), perangkat lunak (*software*), dan perangkat keras (*hardware*).

e. **Blok Basis Data.** Basis data (*database*) merupakan kumpulan dari data yang saling berhubungan satu dengan yang lainnya, tersimpan di perangkat keras komputer dan digunakan perangkat lunak untuk memanipulasinya.

f. **Blok Kendali**. Beberapa pengendalian perlu dirancang dan diterapkan untuk meyakinkan bahwa hal-hal yang dapat merusak sistem dapat dicegah bila terlanjur terjadi kesalahan-kesalahan dapat langsung cepat diatasi.

### 2.2.4. Pengertian Teknologi Informasi

Teknologi Informasi adalah suatu *hardware* dan *software* yang digunakan oleh sistem informasi, hardware atau perangkat keras merupakan peralatan fisik yang terlibat dalam pemrosesan informasi seperti *computer, workstation*, peralatan jaringan, tempat penyimpanan data serta peralatan transmisi. TI adalah memproses dan menyimpan informasi, sama baiknya dengan teknologi komunikasi untuk transmisi informasi.

## 2.3. Audit Sistem Informasi

Audit sistem informasi adalah cara untuk melakukan pengujian terhadap sistem informasi yang ada di dalam organisasi untuk mengetahui apakah system informasi yang dimiliki telah sesuai dengan visi, misi dan tujuan organisasi, menguji performa sistem informasi dan untuk mendeteksi risiko-risiko dan efek potensial yang mungkin timbul. Jadi, Audit Sistem Informasi merupakan mekanisme yang umum digunakan untuk memeriksa dan mengevaluasi

implementasi sistem tata kelola TI. Dalam hal ini pemeriksa (auditor) memegang peran penting dalam hal penilaian dan pengukuran terhadap dewan direksi dan manajemen eksekutif.[6]

### 2.3.1. Tipe – Tipe Pendekatan Audit Sistem Informasi

Perkembangan teknologi informasi, perangkat lunak, sistem jaringan dan komunikasi dan otomatisasi dalam pengolahan data berdampak perkembangan terhadap pendekatan audit yang dilakukan, tiga pendekatan yang dilakukan oleh auditor dalam memeriksa laporan keuangan klien yang telah mempergunakan Sistem Informasi Akuntansi.[7]

a. *Auditing Around The Computer*. Pendekatan ini merupakan pendekatan yang mula-mula ditempuh oleh auditor. Dengan pendekatan ini komputer yang digunakan oleh perusahaan diperlakukan sebagai *Black Box*. Asumsi yang digunakan dalam pendekatan ini adalah bila sampel *output* dari suatu sistem ternyata benar berdasarkan masukan sistem tadi, maka pemrosesannya tentunya dapat diandalkan. Dalam pemeriksaan dengan pendekatan ini, audito*r* melakukan pemeriksaan di sekitar komputer saja.
b. *Auditing With The Computer*. Pendekatan ini digunakan untuk mengotomatisati banyak kegiatan audit. Auditor memanfaatkan komputer sebagai alat bantu dalam melakukan penulisan, perhitungan, pembandingan dan lainnya. Pendekatan menggunakan perangkat lunak *Generalized Audit Software*, yaitu program audit yang berlaku umum untuk berbagai klien.
c. *Auditing Through The Computer*. Pendekatan ini lebih menekankan pada langkah pemrosesan serta pengendalian program yang dilakukan oleh sistem

komputer. Pendekatan ini mengasumsikan bahwa jika program pemrosesan dirancang dengan baik dan memiliki aspek pengendalian yang memadai. .pendekatan ini biasanya diterapkan pada sistem pengolahan data *on-line* yang tidak memberikan jejak audit yang memadai.

### 2.3.2. Metodologi Audit Sistem Informasi

Dalam pelaksanaanya, auditor sistem informasi atau TI mengumpulkan bukti-bukti yang memadai melalui berbagai teknik termasuk *survey*, wawancara, observasi dan *review* dokumentasi. Biasanya, auditor menerapkan teknik CAAT *(Computer Aided Auditing Technique).* Teknik ini digunakan untuk menganalisa data, misalnya saja data pendaftaran pasien RJ, pendaftaran pasien askes, dan lain-lain. Dalam menjalankan proses audit, harus *Audit planning* (perencanaan audit) yang jelas menerangkan tujuan audit, kewenangan auditor, adanya persetujuan managemen tinggi, dan metode audit. Metodologi audit adalah :

1. *Audit subject*. (apa yang akan di-audi) dan *Audit objective* (tujuan audit).
2. *Audit Scope.* Menentukan sistem, fungsi, dan bagian dari organisasi yang secara spesifik atau khusus akan di-audit.
3. *Preaudit Planning.* Mengidentifikasi sumber daya yang dibutuhkan, dokumen yang diperlukan untuk menunjang audit, menentukan lokasi audit.
4. *Audit procedures and steps for data gathering.* Menentukan cara audit untuk memeriksa dan menguji kendali, menentukan siapa yang akan diwawancara.
5. Evaluasi hasil pengujian dan pemeriksaan. Spesifik tiap organisasi.
6. Prosedur komunikasi dengan pihak manajemen.

7. *Audit Report Preparation.* Menentukan bagaimana cara memeriksa hasil audit, yaitu evaluasi kesahihan dokumen, prosedur, dan kebijakan organisasi yang di-audit. Struktur dan isi laporan audit umumnya terdiri atas :

   a. Pendahuluan. Tujuan, ruang lingkup, lamanya audit, prosedur audit & Kesimpulan umum dari auditor.
   b. Hasil audit. Hasil audit, apakah prosedur dan kontrol layak atau tidak, & Rekomendasi. Tanggapan dari manajemen (bila perlu).
   c. *Exit interview*. *Interview* akhir antara auditor dengan pihak manajemen untuk membicarakan temuan dan rekomendasi tindak lanjut.

### 2.3.3. Tahapan Audit Sistem Informasi

Proses audit sistem informasi dapat terdiri dari enam langkah.[2]

1. **Perencanaan**. Tujuan dari perencanaan audit adalah langkah awal menentukan tujuan dan ruang lingkup dari pemeriksaan, seperti : *audit objective.* Menentukan tujuan dari audit, dan *audit Scope.* Ruang lingkup yang dimaksud adalah area, fungsi dan unit organisasi yang akan di-audit mencakup sistem secara spesifik, fungsi atau unit organisasi yang menjadi tujuan (fokus) dari proses audit untuk meminimalkan resiko bisnis.
2. **Pelaksanaan dan Dokumentasi.** Di dalam tahap ini auditor akan mengumpulkan semua data dan informasi yang bisa dikumpulkan untuk menunjang penganalisisan risiko dan menentukan risiko yang mana sampai saat ini tidak ditangani dengan benar.

3. **Penemuan dan Validasi.** Tahap ini, auditor selanjutnya melakukan audit uji kepatutan (*compliance test*) proses TI yang berlangsung terhadap standar dan regulasi yang berlaku. Proses ini akan menemukan temuan-temuan yang nantinya sebagai bahan rekomendasi. Melakukan validasi temuan dan dikonfirmasikan kepada orang yang menanganinya atau bagian terkait.

4. **Mencari Solusi**. Apabila auditor telah menemukan potensial *issues* dan telah memvalidasikan hal yang terkait, maka langkah selanjutnya adalah mencari solusi untuk menanggulangi dan mengantisipasi risiko yang dapat terjadi seperti menilai tingkat kedewasaan proses teknologi informasi yang berlangsung pada suatu organisasi.

5. **Laporan.** Tahap terakhir pada pelaksanaan lapangan adalah membuat laporan audit. Sebelum laporan ini dikeluarkan, auditor harus memberikan laporan sementara kepada bagian terkait untuk persetujuannya.

6. **Tindak Lanjut.** Rekomendasi yang telah disetujui tidak akan berguna apabila tidak diimplementasikan atau tidak dengan benar implementasinya.




**Gambar 2.1**. **Tahapan Audit**
**(Sumber : Evaluasi Pengontrolan Sistem Informasi [2])**

### 2.3.4. *Auditing* Teknologi Informasi

Audit teknologi informasi adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi ini dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis. Pada mulanya istilah ini dikenal dengan audit pemrosesan data elektronik, dan sekarang audit teknologi informasi secara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan itu. Istilah lain dari audit teknologi informasi adalah audit komputer yang banyak dipakai untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya.

## 2.4. Sistem Informasi Manajemen Rumah Sakit

Sistem Informasi Manajemen adalah sistem informasi yang digunakan untuk menyajikan informasi yang digunakan dalam mendukung operasi, manajemen, dan pengambilan keputusan dalam sebuah organisasi. Biasanya SIM menyediakan informasi untuk operasi organisasi.[8] Manajemen rumah sakit adalah serangkaian kegiatan manajemen dari tahap perencanaan sampai tahap evaluasi yang berorientasi pada aspek input (pelanggan, dokter, sarana, prasarana dan peralatan), proses (pelayanan medik) dan output (kepuasan pasien).[9]

Sistem Informasi Rumah Sakit (SIRS) adalah suatu tatanan yang berurusan dengan pengumpulan data, pengelolaan data, penyajian informasi, analisis dan penyimpulan informasi serta penyampaian informasi yang dibutuhkan untuk kegiatan rumah sakit. SIRS ini meliputi : sistem informasi klinik, sistem informasi

administrasi dan sistem informasi manajemen. Peran SIRS yang utama adalah dalam mendukung pengendalian mutu pelayanan medis, penilaian produktivitas, analisis pemanfaatan dan perkiraan kebutuhan, perencanaan dan evaluasi program, menyederhanakan pelayanan, penilaian klinis dan serta pendidikan.[10]

Sistem Informasi Manajemen Rumah Sakit merupakan himpunan atau kegiatan dan prosedur yang terorganisisasikan dan saling berkaitan serta saling ketergantungan dan dirancang sesuai dengan rencana dalam usaha menyajikan info yang akurat dan tepat waktu di rumah sakit. SIM-RS berguna untuk menunjang proses fungsi-fungsi manajemen dan pengambilan keputusan dalam memberikan pelayanan kesehatan di rumah sakit dan juga untuk menunjang fungsi perencanaan dan evaluasi. Dari penampilan kerja rumah sakit antara lain adalah jaminan mutu pelayanan rumah sakit yang bersangkutan, pengendalian keuangan dan perbaikan hasil kerja rumah sakit tersebut, kajian dalam penggunaan dan penaksiran permintaan pelayanan kesehatan rumah sakit oleh masyarakat, perencanaan dan evaluasi program RS, penyempurnaan laporan rumah sakit serta untuk kepentingan pendidikan dan pelatihan.[10]

## 2.5. *Framework* COBIT 4.1

COBIT dikembangkan oleh *IT Governance Institute* (ITGI), yang merupakan bagian dari (ICASA). COBIT *(Control Objectives for Information and Related Technology)* adalah sebuah *framework* dan alat pendukung yang membantu manajer menjembatani *gap* antara tujuan untuk keperluan pengendalian, permasalahan teknik *(technical issue)* dan risiko bisnis serta mengkomunikasikan level pengendalian kepada *stakeholders*.[11, p. 5] COBIT

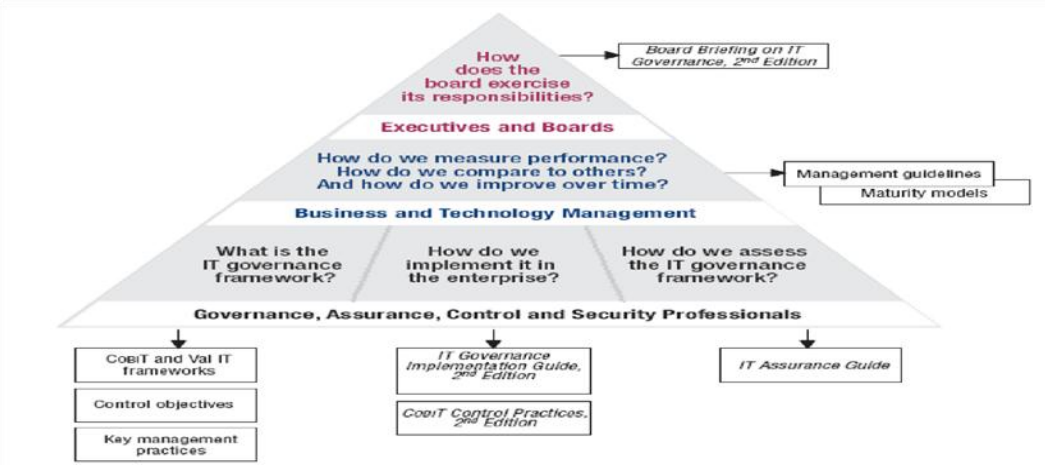
membantu menyokong pengembangan kebijakan yang jelas dan langkah-langkah praktis terbaik yang dapat diambil untuk pengendalian teknologi informasi di seluruh perusahaan. Pengelolaan a*ssurance*, pengendalian dan *security professionals*. COBIT 4.1 menyediakan langkah-langkah praktis terbaik yang dapat diambil dan lebih difokuskan pada pengendalian *(control),* yang selanjutnya dijelaskan dalam domain dan *framework* proses.

COBIT *(Control Objective for Information related Technology)* mengintegrasikan praktik-praktik yang baik dalam mengelola Teknologi Informasi (TI) dan menyediakan kerangka kerja untuk tata kelola TI yang dapat membantu pemahaman dan pengelolaan risiko serta memperoleh keuntungan terkait dengan TI. Keuntungan yang diperoleh dari penerapan COBIT 4.1.[11]

1) Penyelarasan yang lebih baik, berdasarkan pada fokus bisnis.
2) Dapat dipahami oleh manajemen tentang hal yang dilakukan TI.
3) Tanggung jawab dan kepemilikan yang jelas didasarkan orientasi proses.
4) Dapat diterima secara umum diantara pihak ketiga dan pembuat aturan.
5) Berbagi pemahaman diantara pihak yang berkepentingan, didasarkan pada sebuah bahasa yang sama.
6) Pemenuhan kebutuhan sebagai pelengkap COSO *(Committee of Sponsoring Organisations of the Treadway Commision)* untuk lingkungan kendali TI.

Prinsip dasar *framework* COBIT 4.1 adalah untuk menyediakan informasi yang diperlukan dalam mewujudkan tujuan perusahaan atau organisasi. Contohnya mengelola dan mengendalikan sumber daya TI dengan menggunakan sekumpulan proses TI yang terstruktur sehingga dapat memberikan layanan

informasi yang dibutuhkan.[11] Kesemua kandungan yang terdapat pada COBIT, di rangkum dalam gambar di bawah ini :

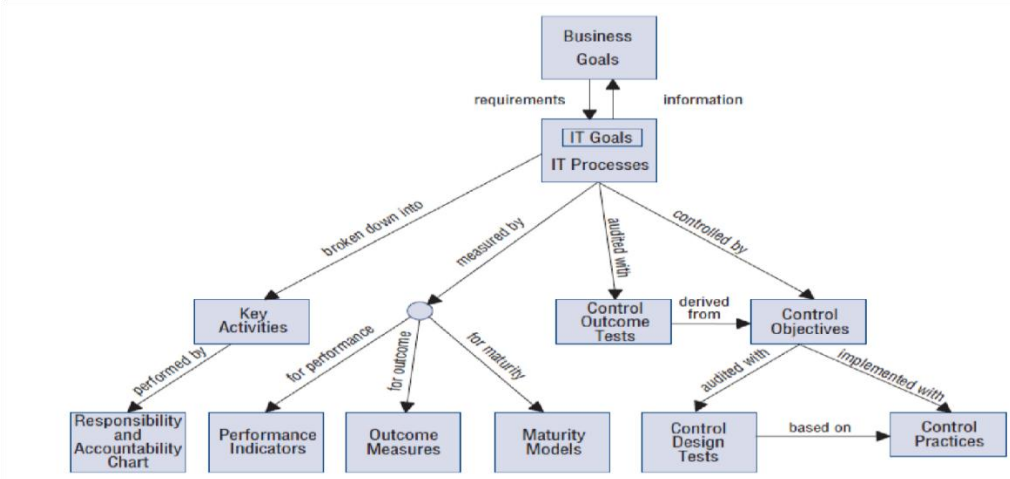



**Gambar 2.2. *Content Diagram* COBIT 4.1**
**(Sumber : *IT Governance Institute, COBIT* 4.1 [11])**

1. *Board Briefing on IT Governance, 2nd Edition* . Membantu para eksekutif memahami betapa pentingnya *IT Governance*, apa yang menjadi masalah dan tanggung jawab mereka dalam pengelolaannya.
2. *Management guidelines/maturity models* . Membantu menentukan tanggung jawab, pengukuran kinerja, tolak ukur dan menemukan *gap* kapabilitasnya.
3. *Frameworks*. Mengorganisasikan objektif *IT Governance* dan *good practices* pada *domain* dan proses IT serta menghubungkannya dengan kebutuhan bisnis.
4. *Control Objectives.* Menyediakan sebuah kumpulan komplit dari kebutuhan tingkat tinggi yang akan dipertimbangkan oleh manajemen guna mengendalikan setiap proses IT agar lebih efektif.

5. *IT Governance Implementation Guide: Using COBIT® and Val IT TM, 2nd Edition* . Menyediakan peta jalan yang umum untuk mengimplementasikan *IT governance* dengan menggunakan COBIT dan Val IT TM *Resources*.
6. *COBIT ® Control Practices: Guidance to Achieve Control Objectives for Sucessful IT Governance, 2nd Edition.* Menyediakan petunjuk mengenai mengapa kontrol sangat penting untuk perlu diimplementasikan dan bagaimana untuk mengimplementasikannya.
7. *IT Assurance Guide: Using COBIT ®*. Menyediakan pedoman mengenai bagaimana COBIT 4.1 dapat digunakan untuk mendukung jaminan dari keanekaragaman aktifitas bersama dengan langkah pengujian yang diusulkan dalam proses IT dan objektif kontrol.

Semua Komponen COBIT 4.1 ini saling berhubungan, memberikan dukungan untuk pemerintahan, manajemen, kontrol dan jaminan kebutuhan audiens yang berbeda, seperti yang ditunjukan pada gambar berikut :




**Gambar 2.3.** ***Interrelationships of COBIT* 4.1 *Components***
***(*Sumber *: IT Governance Institute , COBIT 4.1thed* [11, p.8] *)***

Orientasi bisnis dari COBIT 4.1 adalah menghubungkan tujuan bisnis ke dalam tujuan teknologi informasi yang mana di hubungkan dengan adanya IT Proses. Jadi, proses IT harus dilakukan pengendalian dengan menggunakan *control objectives* yang dimiliki COBIT. Dari *control objectives* ini, akan di pecah lagi menjadi *audit guidelines* pada penjabaran dan penterjemahan *control objectives* dan *control practices* sebagai implementasi dari *control objectives.* Prinsip dasar dari *framework* COBIT adalah untuk menyediakan informasi yang diperlukan untuk mencapai tujuan perusahaan. IT Proses juga dijabaran terhadap pengukuran yang didefinisikan berikut :

1. ***Maturity Model* :** Untuk memetakan status maturity proses-proses IT (dalam *scoring* 0-5) dibandingkan dengan *"the best in class in the industry"* dan juga *International Best Practise.*
2. ***Critical Success Factors (CSFs)*** : Berisi arahan implementasi bagi manajer agar dapat melakukan *control* atas proses TI.
3. ***Key Goal IndicatorsH (KGIs)*** : Berisi kinerja proses-proses TI sehubungan dengan kebutuhan bisnis.
4. ***Key Performance Indicators (KPIs)*** : Kinerja proses-proses TI sehubungan dengan proses-proses pencapaian tujuan.

### 2.5.1. *Focus Area* Tata Kelola TI COBIT 4.1

Focus area tata kelola teknologi informasi dibagai menjadi 5 bagian yaitu *Strategic alignment, Value delivery, Resource management, Risk management, and Performance measurement*. Digambarkan seperti **gambar 2.4** dibawah ini:




**Gambar 2.4. *Focus area IT Governance COBIT 4.1***
**(Sumber : *IT Governance Institute, COBIT 4.1* [11])**

1. *Strateggic Aligment:* Memastikan keterkaitan antara bisnis dengan ketentuan rencana teknologi informasi, pemeliharaan serta validasi usulan nilai teknologi informasi, dan menyelaraskan tujuan bisnis dan tujuan teknologi informasi.
2. *Value delivery*: Menjalankan proposisi nilai seluruh siklus *delivery*, memastikan bahwa TI memberikan manfaat sesuai tujuan bisnis yang dituangkan dalam strategi, dan membuktikan nilai intrinsik dari TI.
3. *Resource management*: Tentang investasi yang optimal dalam pengelolaan sumber daya teknologi informasi : aplikasi, informasi, infrastruktur dan SDM dan pengoptimalisasian infrastruktur.
4. *Risk management:* Tentang kesadaran mengelola risiko, bagaimana memahami persyaratan kepatuhan, keterbukaan tentang risiko yang signifikan dan menanamkan tanggung jawab manajemen risiko ke dalam organisasi.
5. *Performance measurement:* Pengukuran kinerja dan *track* implementasi strategi, penyelesaian proyek, penggunaan sumber daya, kinerja proses dan

pelayanan, misalnya, *balanced scorecard* yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan yang terukur.

### 2.5.2. Para Pengguna *(Audit Guidelines)* Dalam COBIT 4.1

COBIT dibuat untuk dijadikan pegangan oleh para pengguna berikut ini :

*a.* ***Management.*** Dibuat dengan tujuan guna membantu mereka dalam menyeimbangkan risiko dan pengendalian investasi di dalam sebuah lingkungan IT yang sering sifatnya tidak dapat diprediksi *(unpredictable).*

*b.* ***End-User*** **(para pemakai akhir).** Dirancang dengan tujuan memperoleh saran pengamanan dan pengendalian jasa layanan IT yang diberikan atau disediakan oleh pihak internal perusahaan maupun pihak ketiga.

*c.* ***Auditor***. Dibuat dengan tujuan memperkuat opini audit dan memberikan masukan, saran untuk manajemen dalam pengendalian internal.

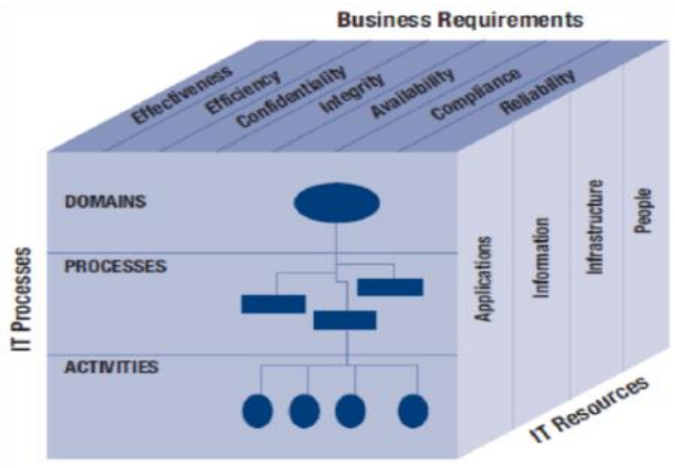
### 2.5.3. Karakteristik Utama *Framework* COBIT 4.1

Secara keseluruhan konsep *framework* COBIT 4.1 digambarkan sebagai sebuah kubus tiga dimensi yang terdiri dari:

(1) kebutuhan bisnis,

(2) sumber daya teknologi informasi dan

(3) proses teknologi informasi. Untuk jelasnya yaitu :




**Gambar 2.5. *The COBIT 4.1 Cube***
**(Sumber : *IT Governance Institute, COBIT 4.1* [11])**

1. *Bussiness Requirements* (Kebutuhan Bisnis). Orientasi pada bisnis menunjukkan bahwa COBIT 4.1 dirancang untuk dapat digunakan oleh banyak pihak seperti user maupun auditor, tetapi lebih penting lagi adalah sebagai panduan yang komprehensif bagi manajemen dan pemilik proses bisnis. Tujuh kriteria informasi yang menjadi perhatian COBIT 4.1 adalah :

a) *Effectiveness*, berhubungan dengan informasi yang relevan dan berhubungan pada proses bisnis seperti halnya disampaikan dengan suatu cara yang tepat waktu, benar, konsisten, dan mudah digunakan.

b) *Efficiency,* berhubungan dengan ketentuan informasi melalui penggunaan sumber daya secara optimal.

c) *Confidentiality*, berhubungan dengan pengamanan informasi yang sensitif dari penyingkapan yang tidak sah.

d) *Integrity*, berhubungan dengan ketepatan dan kelengkapan informasi seperti halnya pada keabsahannya menurut nilai dan harapan bisnis.

e) *Availability*, berhubungan dengan ketersediaan informasi pada saat diperlukan oleh proses bisnis saat ini dan mendatang. Ini juga berhubungan dengan pengamanan sumber daya yang perlu dan kemampuan yang berkaitan.

f) *Compliance*, berhubungan dengan kepatuhan pada hukum, regulasi, perjanjian kontrak dimana proses bisnis adalah pokok yaitu kriteria bisnis dikenakan secara eksternal, seperti halnya kebijakan internal.

g) *Reliability*, berhubungan dengan ketentuan informasi yang tepat bagi manajemen untuk mengoperasikan entitas dan menjalankan *fiduciary*-nya dan tanggung jawab tata kelola.

2. *IT Resources* (Sumber Daya IT). *IT Resource* adalah sumber daya yang berkaitan teknologi informasi . *IT Resource* terdiri dari empat hal yaitu :

a) Aplikasi adalah sistem user yang diotomasikan dan prosedur manual yang memproses informasi.

b) Informasi merupakan data yang diinput, diproses dan dihasilkan oleh sistem informasi yang digunakan untuk kebutuhan bisnis.

c) Infrastruktur merupakan teknologi dan fasilitas (seperti *hardware, operating system, database management systems*, jaringan, multimedia, dan lain-lain) yang mendukung proses aplikasi.

d) *People* (Orang). Merupakan personil yang dilakukan untuk merencanakan, mengorganisasi, memperoleh, mengimplementasi, mendukung memonitor, dan mengevaluasi sistem dan layanan informasi. Personil dapat berasal dari internal perusahaan, *outsource* maupun kontak.

3. *IT Processes* (Proses IT)

Kerangka kerja COBIT4.1 menyediakan referensi pada proses agar setiap orang didalam perusahaan dapat me-*manage* oprasi TI. Aktivitas TI dalam COBIT didefinisikan kedalam model proses yang dikelompokkan kedalam 4 (empat) domain yaitu *Planning and Organise* (PO), *Acquire and Implement* (AI), *Deliver and Support* (DS), *Monitor and Evaluate* (ME).

d. Berbasis Kontrol.

COBIT mendefinisikan kebijakan, prosedur, praktik, dan struktur organisasi yang dirancang untuk memberikan jaminan yang dapat diterima bahwa tujuan bisnis dapat tercapai dan kejadian yang tidak diharapkan dapat dicegah atau diketahui dan diperbaiki dalam suatu kendali *(control).* Agar tata kelola TI menjadi efektif maka diperlukan penerapan kerangka kerja kontrol yang mencakup semua proses TI. Setiap proses TI yang terdapat pada COBIT mempunyai tujuan kontrol tingkat tinggi dan *Detailed Control Objective* (DCO).

5. Dikendalikan Oleh Pengukuran

Pemahaman terhadap status TI diperlukan bagi organisasi untuk kontrol mana yang perlu diberikan dalam upaya meningkatkan kinerjanya. Berkaitan dengan hal tersebut, COBIT memberikan :

a) Model kematangan, yang memungkinkan pembandingan dan identifikasi kapabilitas yang diperlukan.

b) Tujuan dan ukuran kinerja untuk proses TI.

c) Tujuan aktifitas untuk memungkinkan kinerja proses yang efektif.

### 2.5.4. *Maturity Models*

Penilaian kemampuan proses berdasarkan *maturity models* COBIT 4.1 adalah bagian kunci dari implementasi pengelolaan teknologi informasi. Setelah mengidentifikasikan *IT processes* dan *IT controls* yang vital, dengan memodelkan maturity akan dapat diketahui gap yang terdapat di dalam kemampuan *(capability)* perusahaan.[11,p.17) Penggunaan *maturity models* yang dikembangkan untuk setiap 34 proses TI dari COBIT 4.1,[11] memungkinkan manajemen dapat mengidentifikasi :

1) Performa sesungguhnya perusahaan – dimana kondisi perusahaan sekarang atau kondisi *exixting (as is).*
2) Kondisi sekarang dari industri – perbandingan.
3) Target peningkatan perusahaan – dimana kondisi yang diinginkan perusahaan atau kondisi ideal *(to be).*

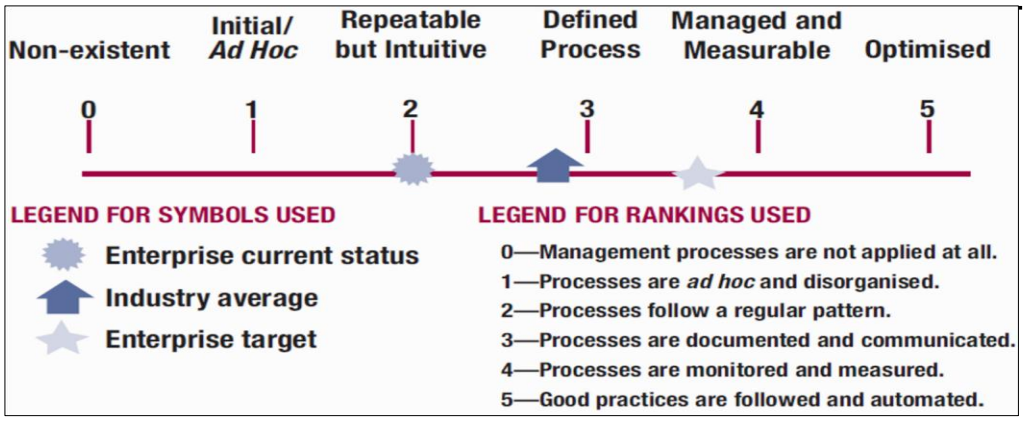
Tujuan pengukuran nilai *maturity level* adalah :

1. Menumbuhkan kepedulian *(awareness)*
2. Melakukan identifikasi kelemahan *(weakness)*
3. Melakukan identifikasi kebutuhan perbaikan *(improvement).*

Model kematangan dimaksudkan untuk mengetahui keberadaan persoalan yang ada dan bagaimana menentukan prioritas peningkatan. Tingkat kematangan COBIT dimulai dari keadaan 0 (tidak ada) hingga 5 (optimal).[11] Penjelasan dari setiap tingkat kematangan COBIT ada pada Tabel 2.1.

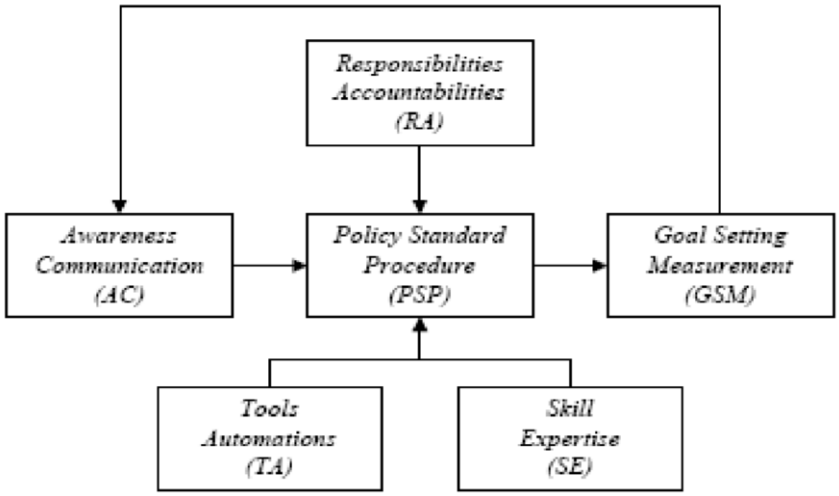
**Tabel 2.1. Tingkat Kematangan Pada COBIT 4.1**
**(Sumber : *IT Governance Institute, COBIT 4.1* [11])**

| Tingkat | Penjelasan |
|---|---|
| 0 | *Non- existent* (tidak ada), merupakan posisi kematangan terendah, dimana organisasi merasa tidak peduli terhadap pentingnya TI untuk dikelola secara baik oleh manajemen. |
| 1 | *Initial*/ *Ad Hoc* (inisialisasi), kondisi dimana organisasi secara reaktif melakukan penerapan implementasi TI sesuai dengan kebutuhan yang ada, tanpa dilakukan perencanaan terlebih dahulu. |
| 2 | *Repeatable but intuitive* (dapat diulang), kondisi dimana organisasi telah memiliki kebiasaan yang terpola untuk merencanakan dan mengelola *IT Governance* dan dilakukan secara berulang-ulang secara reaktif, namun belum melibatkan prosedur dan dokumen formal. |
| 3 | *Defined process* (ditetapkan), pada tahapan ini organisasi telah memiliki mekanisme dan prosedur yang jelas mengenai tata cara dan manajemen *IT Governance*, tersosialisasikan dengan baik di seluruh jajaran manajemen dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari. |
| 4 | *Managed and measurable* (diatur), merupakan kondisi dimana manajemen organisasi telah menerapkan sejumlah indikator pengukuran kinerja kuantitatif untuk memonitor dan mengukur efektivitas pelaksanaan manajemen *IT Governance*. Proses diperbaiki terus menerus dan terdapat perangkat bantu dan otomatisasi untuk pengawasan. |
| 5 | *Optimised* (dioptimalisasi), merupana level kematangan tertinggi, organisasi dianggap telah mengimplementasikan tata kelola manajemen TI yang mengacu pada praktik terbaik (*best practice*). Perbaikan dilakukan terus-menerus sehingga proses telah mecapai level terbaik. |




**Gambar 2.6. *Maturity Models***
**(Sumber : *IT Governance Institute, COBIT4.1* [11])**

*Maturity models* (Kematangan) yang dibangun berawal dari *generic qualitative model*, dimana prinsip dari atribut berikut ditambahkan dengan cara bertingkat yaitu : *Awareness and Communication* (AC), *Policies, Standards and Procedures* (PSP), *Tools and Automation* (TA), *Skills and Expertise* (SE), *Responsibility and Accountability* (RA), *Goal Setting and Measurement* (GSM).[11]




**Gambar 2.7. *Generic Qualitative Model***
**(Sumber : *IT Governance Institute, COBIT 4.1* [11])**

Dari gambar 2.7 secara umum dapat dikatakan bahwa AC merupakan atribut penggerak pertama bagi keberadaan atribut yang lain. AC diwujudkan dalam bentuk PSP, dan untuk terlaksananya PSP dengan baik harus didukung keberadaan atribut lain yaitu TA, SE, dan RA. Adapun pelaksanaan PSP harus senantiasa dimonitor dan diukur terhadap tujuan yang telah ditetapkan dalam GSM. Umpan balik dari GSM diperlukan oleh AC untuk dapat melakukan tindakan evaluasi serta perbaikan yang diperlukan.

Dalam melakukan pengukuran *maturity* untuk proses, terlebih dulu perlu kejelasan tentang tujuan pengukuran itu sendiri. Pemahaman secara jelas, apa yang diukur dan apa yang akan dilakukan pada saat melakukan pengukuran, diperlukan. Hal ini karena pengukuran *maturity (*kematangan) bukan merupakan tujuan tetapi sebagai pendukung untuk Meningkatkan kepedulian, Identifikasi kelemahan dan prioritas peningkatan.[12] Beberapa cara yang umum dilakukan dalam melaksanakan penilaian *maturity* diantaranya :

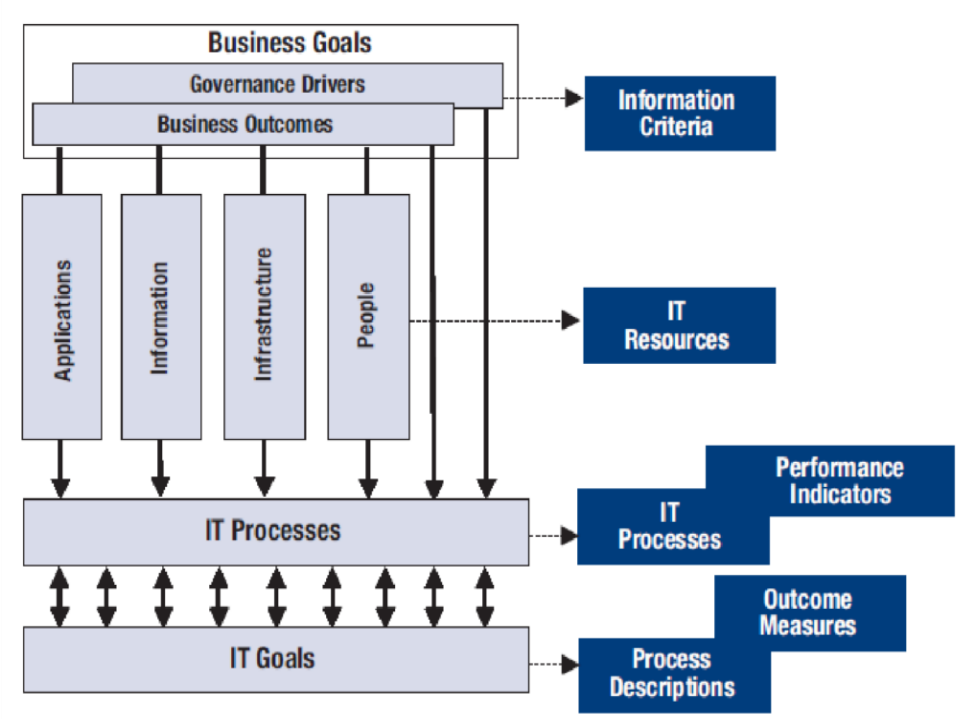
1) Pendekatan multidisiplin kelompok orang yang mendiskusikan dan menghasilkan kesepakatan *maturity level* dari kondisi sekarang.

2) Dekomposisi deskripsi *maturity* menjadi beberapa statement sehingga manajemen dapat memberikan tingkat persetujuannya.[13]

3) Penggunaan atribut matriks sebagaimana didokumentasikan dalam *COBIT's Management Guidelines* dan memberikan nilai masing-masing atribut dari setiap proses.

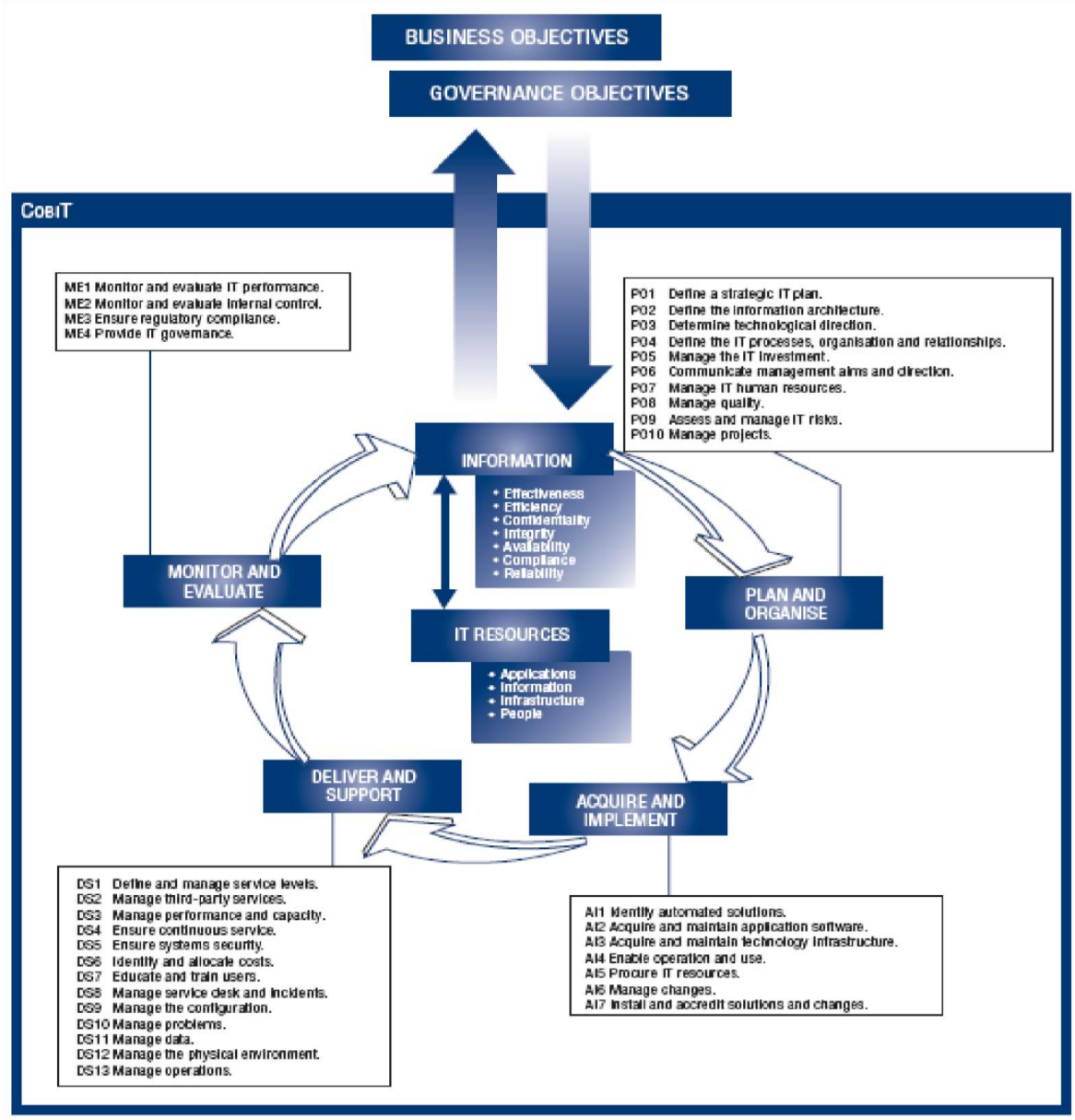
### 2.5.5. Model *Framework* COBIT 4.1

Model proses COBIT 4.1 memungkinkan *IT activities* dan sumberdaya yang mendukungnya dikelola dan dikontrol dengan tepat berdasarkan *COBIT's control objectives*, serta diselaraskan dan dimonitor menggunakan *COBIT's KGI and KPI metrics*, sebagaimana pada gambar 2.8 berikut :




**Gambar 2.8.** ***COBIT 4.1 Management, Control, Alignment and Monitoring***
**(Sumber :** ***IT Governance Institute, COBIT 4.1*** **[11])**

Secara lebih terinci keseluruhan *framework* COBIT 4.1 ditunjukkan sebagaimana pada gambar 2.9, dengan COBIT's *process model* dari empat domain mengandung 34 proses generik, yang mengelola *IT resources* untuk memberikan informasi bisnis sesuai dengan kebutuhan bisnis dan tata kelola TI.




**Gambar 2.9. *Framework COBIT 4.1***
**(Sumber : *IT Governance Institute, COBIT 4.1* [11])**

1. *Audit Guidelines*

Fungsinya adalah memberikan atau menyediakan perangkat struktur yang sederhana dan *simple* guna proses *auditing* dan penilaian pengendalian berdasarkan praktik-praktik audit yang diterima secara umum yang sesuai dalam *framework* COBIT secara keseluruhan.

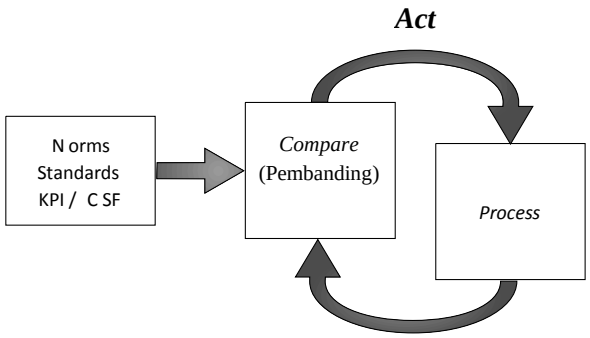
**Tabel.2.2. Detail struktur *Audit Guidelines* Aplikasi Pada COBIT 4.1 (Sumber : *IT Governance Institute, COBIT 4.1* [11])**

| | |
|---|---|
| **Level 1**<br>General IT audit approach | ı COBIT *Framework*<br>ı Audit Process Requirements<br>ı Control Observations<br>ı Generic Audit Guideline |
| **Level 2**<br>Process audit guidelines | ı Detailed *Audit Guidelines* |
| **Level 3**<br>Audit attention points to complement detailed control objectives | ı Local Conditions<br>• sector specific criteria<br>• industry standards<br>• platform specific elements<br>• detailed control techniques used |

**A. Pendekatan umum *Audit* IT *(General IT audit approach)***

a) Persyaratan Proses Audit *( Audit Process Requirements ).* menentukan strategi audit atas dasar rencana audit yang rinci harus dijabarkan lebih lanjut, misalnya, adalah salah satunya untuk pendekatan berbasis atau pendekatan substantif kontrol. Jadi, semua langkah, tugas dan poin keputusan untuk melaksanakan audit perlu dipertimbangkan.

b) Proses Pengendalian Observasi *(Control Process Observations).* Prinsip-prinsip umum pengendalian juga dapat menyediakan wawasan tambahan tentang bagaimana untuk lebih melengkapi. Proses kontrol terdiri dari 4 langkah. Pertama, standar kinerja yang diinginkan ditentukan untuk Proses. Kedua, ada cara merasakan apa yang terjadi dalam proses. Ketiga, kontrol Unit membandingkan informasi dengan standar. Keempat, jika apa yang sebenarnya terjadi tidak sesuai standar, seperti gamabar berikut ini :




**Gambar 2.10. *Control Process Observations***
***(*Sumber : *IT Governance Institute, COBIT 4.1* [11])**

c) Pedoman *Audit Generik (Generic Audit Guidelines)*. langkahnya yaitu :

1) Memperoleh sebuah pemahaman *(Obtaining An Understanding)*

Wawancara manajemen dan staf yang tepat untuk memperoleh pemahaman yaitu tentang Bisnis persyaratan dan risiko yang terkait, Struktur Organisasi, Peran dan tanggung jawab, Kebijakan dan prosedur, Hukum dan peraturan, Langkah-langkah pengendalian, pelaporan Manajemen (status, kinerja, item tindakan). Mendokumentasikan sumber- proses terkait IT terutama dipengaruhi oleh proses yang sedang diperiksa. Konfirmasi pemahaman dari proses laporan. *Key Performance Indicator* (KPI) dari proses, dan implikasi kontrol.

2) Mengevaluasi Kontrol (*Evaluating The Controls*)

Mengevaluasi kesesuaian tindakan pengendalian untuk proses dikaji dengan mempertimbangkan kriteria bisa diidentifikasi dan standar praktek industri, Faktor Kritis Sukses (CSF) dari tindakan kontrol dan menerapkan penilaian profesional auditor yaitu ada proses terdokumentasi, kiriman yang tepat, Tanggung jawab dan akuntabilitas yang jelas dan efektif, ada kontrol

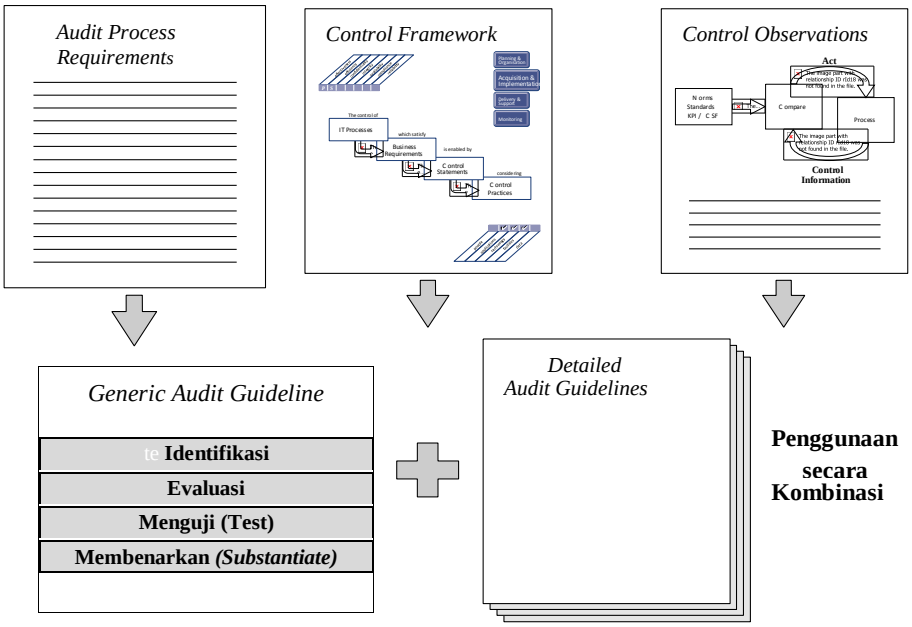
kompensasi ada, bila perlu menyimpulkan sejauh mana tujuan pengendalian terpenuhi.

3) Menilai Kepatuhan (*Assessing Compliance*)

Langkah-langkah pemeriksaan yang akan dilakukan untuk memastikan bahwa tindakan pengendalian bisa bekerja seperti yang ditentukan, secara konsisten dan terus-menerus dan untuk menyimpulkan pada kesesuaian pengendalian lingkungan. Memperoleh bukti langsung atau tidak langsung untuk item yang dipilih untuk memastikan prosedur telah dipenuhi untuk periode laporan menggunakan kedua bukti langsung dan tidak langsung. Menentukan tingkat pengujian substantif dan pekerjaan tambahan untuk memberikan jaminan proses TI yang memadai.

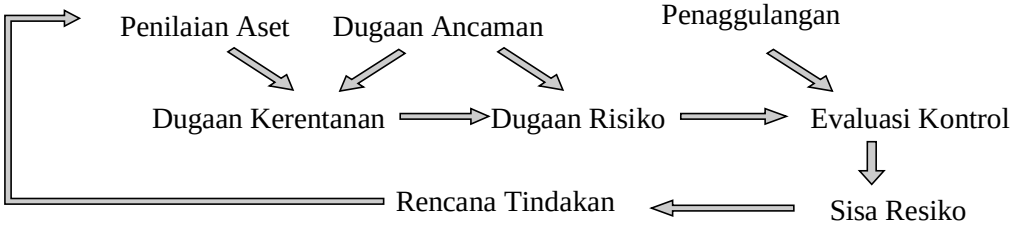
4) Menguatkan Risiko (*Substantiating The Risk*)

Langkah pemeriksaan yang akan dilakukan untuk mendukung risiko tujuan kontrol tidak terpenuhi dengan menggunakan analisis teknik dan konsultasi sumber-sumber alternatif. Tujuannya adalah untuk mendukung pendapat dan 'kejutan' manajemen ke aksi. Auditor harus kreatif dalam mencari dan menyajikan informasi yang rahasia dan sensitif. Mendokumentasikan kelemahan kontrol, ancaman dan kerentanan. Keseluruhan Detailnya seperti pada gambar berikut ini :




**Gambar**. **2.11.** ***Link Control objectives*** **dan** ***Audit Guidelines***
**(Sumber :** ***IT Governance Institute, COBIT 4.1*** **[11])**

Analisis risiko sebagai sebuah alternatif Penilaian Pendekatan Menyeimbangkan biaya dan risiko yaitu, membuat pilihan sadar akan tentang bagaimana dan apakah untuk menerapkan masing-masing tujuan kontrol. Tujuan pengendalian harus diterapkan di suatu tempat untuk mencapai suatu kriteria kontrol informasi (efektivitas, efisiensi, kerahasiaan, ketersediaan, integritas, kepatuhan dan kehandalan). Gambar Pendekatan umum analisis risiko IT yaitu :




**Gambar 2.12. Kerangka Analisis Risiko**
**(Sumber :** ***IT Governance Institute***, ***COBIT 4.1*** **[11])**

2. *Control Objectives*

*Control objectives* TI adalah pernyataan mengenai hasil atau tujuan yang harus dicapai melalui penerapan prosedur kendali dalam aktivitas TI tertentu. Terdiri dari 4 tujuan pengendalian tingkat tinggi *(high-level control objectives)* yang tercermin dalam 4 domain, yaitu :

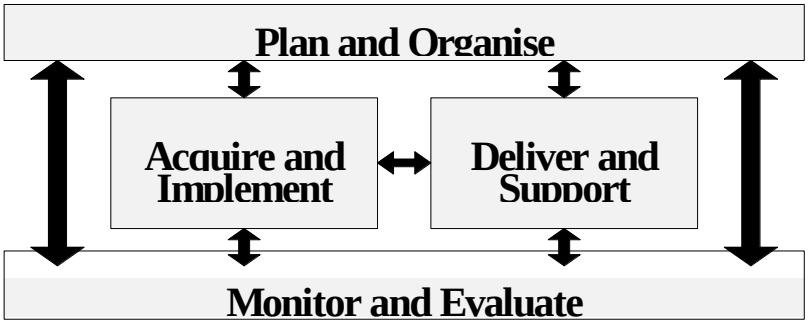
a) *Plan and Organise* (PO), mencakup strategi dan taktik, perhatian pada identifikasi cara TI dapat berkontribusi pada pencapaian objektif bisnis.

b) *Acquire and Implement* (AI), merealisasikan strategi TI yang sudah direncanakan, beserta solusi TI yang diperoleh, diimplementasikan dan diintegrasikan ke dalam proses bisnis organisasi.

c) *Deliver and Support* (DS), domain ini menitik beratkan pada dukungan dan layanan teknologi informasi pada bisnis, mulai dari penanganan keamanan, kesinambungan, dukungan bagi pengguna & manajemen data.

d) *Monitor and Evaluate* (ME). Pada domain ini akan ditekankan kepada pentingnya semua proses TI perlu diakses secara berkala untuk menjaga kualitas dan kesesuaian dengan standar yang telah ditetapkan baik pengawasan, penilaian, dan evaluasi agar proses TI berjalan dengan baik.

Keterkaitan keempat domain COBIT dapat dilihat dalam **gambar 2.13.**




**Gambar 2.13. Keterkaitan Domain dalam COBIT**
**(Sumber : *IT Governance Institute, COBIT 4.1* [11])**

3. *Management Guidelines*

Berisi arahan, baik secara umum maupun spesifik, mengenai apa saja yang mesti dilakukan, terutama agar dapat menjawab pertanyaan- pertanyaan. Konsep dari framework COBIT 4.1 adalah pengendalian terhadap SI dapat dilakukan dengan cara menentukan informasi yang dibutuhkan untuk mendukung *business objectives*. Mendukung dalam pengendalian SI terkait dalam proses sistem informasi yang didukung oleh *(IT Resource).* Arahan ini untuk tujuan bisnis pada proses TI dan mengukur tingkat kepentingan berdasarkan COBIT 4.1.

## 2.6. Model *Balanced Scorecard (BSC)*

*Balanced Scorecard* merupakan suatu alat pengukur kinerja perusahaan yang mengukur kinerja perusahaan secara keseluruhan, baik secara keuangan maupun nonkeuangan dengan menggunakan empat perspektif yaitu, perspektif keuangan, perspektif pelanggan, perspektif bisnis internal, dan perspektif pertumbuhan dan pembelajaran. *Balanced Scorecard* (BSC) dapat mengintegrasikan berbagai pandangan tentang perencanaan, implementasi dan pengukuran strategi organisasi ke dalam empat perspektif .[14]

**Tabel 2.3. Empat Perspektif dalam *Balanced Scorecard* (*BSC)***
**(*Sumber* : *Balanced Scorecard* (BSC) [14] )**

| Perspektif | Misi |
|---|---|
| Pelanggan | Mencapai misi dengan menyampaikan nilai kepada pelanggan. |
| Keuangan | Sukses secara finansial dengan menyampaikan nilai kepada pemegang saham. |
| Proses Bisnis Internal | Memuaskan pemegang saham dan pelanggan dengan meningkatkan efisiensi dan ke efektifan proses bisnis. |
| Pembelajaran dan Pertumbuhan | Mencapai visi dengan mempertahankan inovasi dan mengubah kapabilitas, melalui perbaikan *continue* dan persiapan menghadapi masa depan. |

Keunggulan pendekatan *Balanced Scorecard* (BSC) dalam system perencanaan strategik adalah mampu menghasilkan rencana strategik yang memiliki karakteristik, [14]

a. **Komprehensif**. Perluasan perspektif rencana strategik yaitu perspektif keuangan, pelanggan, proses bisnis internal, serta pembelajaran dan pertumbuhan.

b. **Koheren**. sistem perencanaan strategik memotivasi personel untuk bertanggung jawab.

c. **Seimbang.** sasaran strategik menghasilkan kinerja keuangan berjangka panjang.

d. **Terukur**. sistem perencanaan strategik menjanjikan ketercapaian berbagai sasaran strategik yang dihasilkan oleh sistem tersebut.