

BAB 2

LANDASAN TEORI

2.1. Evaluasi

Menurut Husni (2010), evaluasi adalah suatu proses untuk menyediakan informasi mengenai hasil penilaian atas permasalahan yang ditemukan.

Menurut Umar (2005, p36), evaluasi adalah suatu proses untuk menyediakan informasi tentang sejauh mana suatu kegiatan tertentu telah dicapai, bagaimana perbedaan pencapaian itu dengan suatu standar tertentu untuk mengetahui apakah ada selisih diantara keduanya, serta bagaimana manfaat yang telah dikerjakan itu bila dibandingkan dengan harapan-harapan yang ingin diperoleh.

Menurut Kamus Besar Bahasa Indonesia (2008), evaluasi adalah proses penilaian yang sistematis, mencakup pemberian nilai, atribut, apresiasi, pengenalan permasalahan dan pemberian solusi atas permasalahan yang ditemukan.

Dari pengertian di atas, maka dapat disimpulkan bahwa evaluasi adalah proses untuk memberikan informasi kepada pihak yang terkait tentang pencapaian suatu kegiatan yang dinilai dengan sistematis berdasarkan suatu standar tertentu.

2.2 Sistem Informasi

2.2.1 Pengertian Sistem Informasi

Menurut O'Brien (2008, p7), mendefinisikan "*Information system can be any organized combination of people, hardware, software, commination*

networks and data resources that collect, transform, disseminates information in a organization.” Artinya adalah sistem informasi adalah suatu kesatuan yang terdiri dari manusia (*brainware*), perangkat keras (*hardware*), perangkat lunak (*software*), jaringan komputer dan sumber daya data yang mengumpulkan dan mendistribusikan informasi di dalam suatu organisasi.

2.2.2 Tujuan dan Fungsi Sistem Informasi

Fungsi sistem informasi bertanggung jawab untuk pengolahan data. Pengolahan data merupakan aplikasi sistem informasi akuntansi yang paling mendasar dalam setiap tujuan organisasi.

Tujuan dari pada sistem informasi ada tiga macam, yaitu:

- a. Fungsi kepengurusan manajemen.
- b. Dasar pengambilan keputusan manajemen.
- c. Pendukung kegiatan operasi perusahaan.

2.3 Audit Sistem Informasi

2.3.1 Pengertian Audit Sistem Informasi

Menurut Gondodiyoto (2007, p443), audit sistem informasi dimaksudkan untuk mengevaluasi tingkat kesesuaian antara sistem informasi dengan prosedur bisnis (*bussiness processes*) perusahaan (kebutuhan pengguna, *user needs*) untuk mengetahui apakah sistem informasi telah didesain dan di implementasikan

secara efektif, efisien dan ekonomis, memiliki mekanisme kepengamanan aset, serta menjamin integritas data yang memadai.

Menurut Romney dan Steinbart (2006, p783), *information systems audit reviews the general and application controls of an accounting information system (AIS) to assess its compliance with internal control policies and procedures and its effectiveness in safe guarding assets*. Audit sistem informasi mereview pengendalian umum dan pengendalian aplikasi dari sistem informasi akuntansi untuk menilai ketaatan sistem terhadap kebijakan dan prosedur pengendalian internal serta efektivitas dalam melindungi aset.

Menurut pengertian diatas maka dapat disimpulkan bahwa Audit Sistem Informasi adalah suatu proses mengumpulkan dan mengevaluasi bukti-bukti untuk mengetahui apakah sistem aplikasi sudah menerapkan pengendalian intern yang memadai agar dapat dilindungi dengan baik dan terhindar dari penyalahgunaan.

2.3.2 Tujuan Audit Sistem Informasi

Menurut Romney dan Steinbart (2006, p316) *“The purpose of an information system audit is to review and evaluate the internal control that protect the system.”* Tujuan dari audit sistem informasi adalah untuk mengkaji ulang dan mengevaluasi pengendalian-pengendalian internal yang diterapkan untuk melindungi sistem yang ada.

Ada beberapa tujuan audit sistem informasi menurut Gondodiyoto (2007, p474), yaitu :

1. Pengamanan Aset

Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, *file/data* dan fasilitas lain harus dijaga dengan sistem pengendalian *intern* yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset merupakan suatu hal yang sangat penting yang harus dipenuhi oleh perusahaan.

2. Efektifitas Sistem

Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut sudah dirancang dengan benar (*doing the right thing*), telah sesuai dengan kebutuhan *user*. Informasi yang dibutuhkan oleh para manajer dapat dipenuhi dengan baik.

3. Efisiensi Sistem

Efisiensi menjadi sangat penting ketika sumber daya kapasitasnya terbatas. Jika cara kerja dari sistem aplikasi komputer menurun maka pihak manajemen harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya, karena suatu sistem dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan user dengan sumber daya informasi yang minimal. Cara sistem kerja benar (*doing thing right*).

4. Ketersediaan (*Availibility*).

Berhubungan dengan ketersediaan dukungan atau layanan

teknologi informasi (TI). TI hendaknya dapat mendukung secara *continue* terhadap poses bisnis (kegiatan perusahaan). Makin sering terjadi gangguan (*System Down*) maka berarti tingkat ketersediaan sistem rendah.

5. Kerahasiaan (*Confidentiality*).

Fokusnya ialah pada proteksi terhadap informasi dan supaya terlindungi dari akses dari pihak-pihak yang tidak berwenang.

6. Keandalan (*Realibility*).

Berhubungan dengan kesesuaian dan keakuratan bagi manajemen dalam pengelolaan organisasi, pelaporan dan pertanggungjawaban.

7. Menjaga Integritas Data.

Integritas data (*data integrity*) adalah salah satu konsep dasar dari sistem informasi. Data memiliki atribut-atribut seperti: kelengkapan, kebenaran, dan keakuratan.

2.3.3 Pendekatan Audit Sistem Informasi

Menurut Gondodiyoto (2007, p451), Auditor harus memutuskan pendekatan mana yang akan ditempuh, diantara tiga pendekatan audit yang berkaitan dengan komputer:

1. Audit di sekitar (*input/output*) komputer (*audit around the computer*)

Dalam pendekatan audit di sekitar komputer, auditor (dalam hal ini harus akuntan yang *registered*, dan bersertifikasi akuntan publik) dapat mengambil kesimpulan dan merumuskan opini dengan hanya menelaah struktur pengendalian dan melaksanakan pengujian transaksi dan prosedur verifikasi saldo perkiraan dengan cara sama seperti pada sistem akuntansi

manual. Auditor tidak perlu menguji pengendalian SI berbasis teknologi informasi klien (*file* program atau pengendalian atas *file* atau data di komputer), melainkan cukup terhadap *input* (dokumen) serta *output* (laporan) sistem aplikasi saja.

Keunggulan metode audit di sekitar komputer adalah:

- a. Pelaksanaan audit lebih sederhana.
- b. Auditor yang memiliki pengetahuan minimal di bidang komputer dapat dilatih dengan mudah untuk melaksanakan audit.

Kelemahannya adalah jika kondisi (*user requirements*) berubah, mungkin sistem itupun perlu diredesain dan perlu penyesuaian (*update*) program-program, bahkan mungkin struktur data, sehingga auditor perlu menilai ulang apakah sistem masih berjalan baik.

2. Audit terhadap komputer (*audit through the computer*)

Dalam pendekatan audit ke sistem komputer (*audit through the computer*) auditor melakukan pemeriksaan langsung terhadap program-program dan *file-file* komputer pada audit SI berbasis TI. Auditor menggunakan komputer (*software* bantu) atau dengan cek logika atau *listing* program untuk menguji logika program dalam rangka pengujian pengendalian yang ada pada komputer. Selain itu auditor juga dapat meminta penjelasan dari para teknisi komputer mengenai spesifikasi sistem dan atau program yang diaudit.

Keunggulan pendekatan audit dengan pemeriksaan sistem komputerisasi ialah:

- a. Auditor memperoleh kemampuan yang besar dan efektif dalam melakukan pengujian terhadap sistem komputer
- b. Auditor akan merasa lebih yakin terhadap kebenaran hasil kerjanya.
- c. Auditor dapat menilai kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan.

Sebetulnya mungkin tidak dapat dikatakan sebagai suatu kelemahan dalam pendekatan audit ini, namun jelas bahwa *audit through the computer* memerlukan tenaga ahli auditor yang terampil dalam pengetahuan teknologi informasi, dan mungkin perlu biaya yang besar pula.

3. Audit menggunakan dukungan komputer (*audit with the computer*)

Pada pendekatan ini audit dilakukan dengan menggunakan komputer dan *software* untuk mengotomatisasi prosedur pelaksanaan audit. Pendekatan audit dengan bantuan komputer merupakan cara audit yang sangat bermanfaat, khususnya dalam pengujian substantif atas *file* dan *record* perusahaan. *Software* audit yang digunakan merupakan program komputer yang dipakai auditor untuk membantu pengujian dan evaluasi keandalan *record* atau data perusahaan. Keunggulan menggunakan pendekatan ini adalah:

- a. Merupakan program komputer yang diproses untuk membantu pengujian pengendalian sistem komputer.
- b. Dapat melaksanakan tugas audit yang terpisah dari catatan klien, yaitu dengan mengambil *copy* data atau *file* untuk dites

dengan komputer lain. Kelemahannya adalah upaya dan biaya untuk pengembangan relatif besar.

2.3.4 Jenis Audit Sistem Informasi

Menurut Gondodiyoto (2007, p443), sesungguhnya audit SI berbasis teknologi informasi dapat digolongkan dalam tipe atau jenis-jenis pemeriksaan :

1. Audit laporan keuangan (*general audit on financial statements*)

Dalam hal ini audit terhadap aspek-aspek teknologi informasi pada suatu sistem informasi akuntansi berbasis teknologi adalah dilaksanakan dalam rangka audit keuangan (*general financial audit*) yang sistem akuntansinya berbasis komputer (sering disebut audit teknologi informasi).

Audit *objectives*-nya adalah sama dengan audit tradisional, yaitu memeriksa kesesuaian *financial statements* dengan standar akuntansi keuangan dan ada atau tidak adanya salah saji material pada laporan keuangan.

2. Audit sistem informasi (SI)

Sebagai kegiatan tersendiri, terpisah dari audit keuangan. Sebetulnya audit SI pada hakekatnya merupakan salah satu dari bentuk audit operasional, tetapi kini audit SI sudah dikenal sebagai satu satuan jenis audit tersendiri yang tujuan utamanya lebih untuk meningkatkan IT *governance*.

2.3.5 Tahapan Audit

Tahapan Audit	
Subjek Audit	Tentukan/identifikasi unit/lokasi yang diaudit
Sasaran Audit	Tentukan sistem secara spesifik, fungsi atau unit organisasi yang akan diperiksa
Jangkauan Audit	Identifikasi sistem secara spesifik, fungsi atau unit organisasi untuk dimasukkan lingkup pemeriksaan
Rencana Pre-audit	<ol style="list-style-type: none"> 1. Identifikasi kebutuhan keahlian teknik dan sumber daya yang diperlukan untuk audit. 2. Identifikasi sumber bukti untuk tes atau <i>review</i> seperti fungsi <i>flow chart</i>, kebijakan, <i>standard</i> prosedur dan kertas kerja audit sebelumnya.
Prosedur audit dan langkah-langkah pengumpulan bukti audit	<ol style="list-style-type: none"> 1. Identifikasi dan pilih pendekatan audit untuk memeriksa dan menguji pengendalian intern. 2. Identifikasi daftar individu untuk <i>interview</i>. 3. Identifikasi dan menghasilkan kebijakan yang berhubungan dengan bagian, <i>standard</i> dan pedoman untuk <i>interview</i>. 4. Mengembangkan <i>instrument</i> audit dan metodologi penelitian dan pemeriksaan kontrol internal.
Prosedur untuk evaluasi	<ol style="list-style-type: none"> 1. Organisasikan sesuai kondisi dan situasi. 2. Identifikasi prosedur evaluasi atas tes efektivitas dan efisiensi sistem, evaluasi kekuatan dari dokumen, kebijakan dan prosedur yang diaudit.
Pelaporan hasil audit	Siapkan laporan yang objektif, konstruktif (bersifat membangun) dan menampung penjelasan auditee.

Tabel 2.1 Tahapan Audit

(Sumber: Gondodiyoto (2007, p487))

2.4 Evaluasi Sistem Informasi

2.4.1 Definisi Evaluasi Sistem Informasi

Pada umumnya evaluasi sistem informasi adalah suatu proses menentukan apakah sistem komputer dapat mengamankan aset, memelihara data,

mencapai tujuan organisasi secara efektif melalui pengumpulan dan pengevaluasian bukti - bukti.

Dalam evaluasi sistem informasi kali ini, yang mengambil acuan berdasarkan CobIT 4.1, berdefiniskan mengenai suatu pengendalian yang dapat membantu berbagai kebutuhan manajemen yang berkaitan dengan IT, untuk membantu pengoptimalkan investasi IT, dan menyediakan solusi ketika terjadi penyimpangan serta melakukan penerapan standar keamanan TI yang sesuai dengan kebutuhan manajemen yang ada dalam perusahaan mereka, sehingga meyakinkan bahwa teknologi informasi dan sistem bisnis yang ada telah memadai dalam memelihara integritas data untuk mencapai suatu tujuan yang efisien dan efektif.

2.4.2 Tujuan Evaluasi Sistem Informasi

Sistem informasi (akuntansi) terutama yang berbasis teknologi informasi perlu dievaluasi (atas efektivitas dan efisiensinya) karena berbagai alasan. Alasan pertama adalah karena lazimnya memerlukan dana investasi yang sangat besar. Alasan kedua adalah sistem tersebut melibatkan hampir seluruh posisi kunci dan bahkan mungkin seluruh anggota organisasi. Alasan lain ialah bahwa faktor resiko, kontrol internal, dan dampak kalau terjadi permasalahan akan sangat vital dan kompleks.

Tujuan evaluasi sistem informasi berdasarkan CobIT 4.1 antara lain :

1. Memperoleh nilai dari investasi TI
2. Dapat mengukur sejauh pencapaian IT yang di terapkan
3. Mengurangi resiko – resiko TI yang sering terjadi

4. Meningkatkan efisiensi dan efektifitas kinerja sistem.

2.5 Pengertian Penjualan

Menurut Arif & Wibowo (2008, p.78-79), “Penjualan tunai adalah penjualan barang dagang dengan menerima pembayaran kas atau tunai secara langsung dari pelanggan pada saat terjadinya penjualan.” Sedangkan “ Penjualan Kredit adalah penjualan barang dagang dengan kesepakatan antara pembeli dan penjual pada saat transaksi, yaitu pembayaran akan dilakukan pada waktu yang akan datang.”

2.6 Pengendalian Internal

2.6.1 Definisi Pengendalian Internal

Menurut Rama dan Jones (2008, p.132), “pengendalian internal (*internal control*) adalah suatu proses, yang dipengaruhi oleh dewan direksi entitas, manajemen, dan personel lainnya, yang dirancang untuk memberikan kepastian yang beralasan terkait dengan pencapaian sasaran kategori sebagai berikut : efektifitas dan efisiensi operasi; keandalan pelaporan keuangan; dan ketaatan terhadap hukum dan peraturan yang berlaku.”

Menurut Gondodiyoto (2009,p.133) yang mengutip dari *Information System Audit and Control Association* (ISACA, dalam Cangemi 2003, p.65) menyatakan bahwa internal control adalah : “ *The policies, procedures, practice and organizational structures, design to provide reasonable assurance that*

business objective will be achieved and that undesired events will be prevented, or detected, and corrected. ” Yang dapat didefinisikan sebagai Kebijakan, prosedur, praktek dan struktur organisasi, desain untuk memberikan jaminan yang wajar bahwa tujuan bisnis akan dicapai dan bahwa peristiwa yang tidak diinginkan dapat dicegah, atau terdeteksi, dan dikoreksi.

Gondodiyoto (2009,p.133) yang mengutip dari *The Institute of Internal Auditors (IIA)* adalah : ”*The Attitude and actions of management and the board regarding the significances of control within the organizational. The control environment provides the discipline and structure for the achievement of the primary objectives of the systems of internal control. The control environment includes the following elements: integrity and ethical values, management’s philosophy and operating style, organizational structure, a assignment of authority and responsibility, human resources policies and practices, and competence of personel.*” Yang dapat diartikan sebagai sikap dan tindakan manajemen dan dewan mengenai signifikansi pengendalian dalam organisasi. Lingkungan pengendalian memberikan disiplin dan struktur untuk pencapaian tujuan utama dari sistem pengendalian internal. Lingkungan pengendalian mencakup unsur-unsur berikut: integritas dan nilai-nilai etika, filosofi manajemen dan gaya operasi, struktur organisasi, tugas wewenang dan tanggung jawab, kebijakan dan praktek sumber daya manusia, dan kompetensi pribadi.

2.6.2 Tujuan Pengendalian Internal

Menurut James A.Hall (2007, p.181), Tujuan dari pengendalian internal adalah :

1. Menjaga asset perusahaan.
2. Memastikan akurasi dan kehandalan catatan serta informasi akuntansi.
3. Mendorong efisiensi dalam operasional perusahaan.
4. Mengukur kesesuaian kebijakan serta prosedur yang ditetapkan oleh pihak manajemen.

Sedangkan menurut Gondodiyoto (2007,p260), tujuan disusunnya sistem *control* atau pengendalian internal komputerisasi adalah untuk :

1. Meningkatkan pengamanan (*improve safeguard*) aset sistem informasi (data/catatan akuntansi(*accounting record*) yang bersifat *logical asset*, maupun *physical asset* seperti *hardware, infrastructures*, dan sebagainya).
2. Meningkatkan integritas data (*improve data integrity*),sehingga dengan data yang benar dan konsisten akan dapat dibuat laporan yang benar.
3. Meningkatkan efektivitas sistem (*improve system effectiveness*).
4. Meningkatkan efisiensi sistem (*improve system efficiency*).

2.6.3 Komponen Pengendalian Internal

Menurut Rama and Jones (2006, p104), lima komponen model pengendalian internal adalah:

1. Lingkungan pengendalian

Inti dari bisnis apapun adalah orang-orangnya, ciri perorangan, termasuk integritas, nilai-nilai etika, dan kompetensi serta lingkungan tempat beroperasi. Mereka adalah mesin yang mengemudikan organisasi dan dasar tempat segala hal terletak.

2. Aktivitas pengendalian

Kebijakan dan prosedur pengendalian harus dibuat dan dilaksanakan untuk membantu memastikan bahwa tindakan yang diidentifikasi oleh pihak manajemen untuk mengatasi resiko pencapaian tujuan organisasi, secara efektif dijalankan.

3. Penilaian resiko

Organisasi harus sadar akan dan berurusan dengan resiko yang dihadapinya. Organisasi harus menempatkan tujuan, produksi, pemasaran, keuangan, dan kegiatan lainnya, agar organisasi beroperasi secara otomatis. Organisasi juga harus membuat mekanisme untuk mengidentifikasi, menganalisis, dan mengelola resiko yang terkait.

4. Informasi dan komunikasi

Di sekitar aktivitas pengendalian terdapat sistem informasi dan komunikasi. Mereka memungkinkan orang-orang dalam organisasi untuk mendapat dan bertukar informasi yang dibutuhkan untuk melaksanakan, mengelola, dan mengendalikan operasinya.

5. Pengawasan

Seluruh proses harus diawasi, dan perubahan dilakukan sesuai dengan kebutuhan. Melalui cara ini, sistem dapat beraksi secara dinamis, berubah sesuai tuntutan keadaan.

2.7 CobIT

Menurut Gondodiyoto (2009. P163), “CoBIT adalah sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu auditor, pengguna (*user*), dan manajemen, untuk menjembatani gap antara risiko bisnis, kebutuhan.”

Untuk memenuhi kebutuhan terhadap tujuan bisnis, informasi dibutuhkan untuk memastikan kriteria pengendalian tertentu, CobIT itu sendiri berguna untuk kebutuhan bisnis untuk mendapatkan informasi. Kriteria informasi itu di definisikan sebagai berikut:

1. Efektifitas : berhadapan dengan informasi yang secara relevan dan bersangkutan pada proses bisnis yang juga disampaikan secara tepat waktu, benar, konsisten dan berguna.
2. Efisiensi : bertitik fokus pada ketersediaan informasi secara optimal yang digunakan terhadap sumber daya.
3. Kepercayaan : bertitik fokus terhadap perlindungan informasi yang sensitif dari pihak yang tidak berkepentingan.
4. Integritas : berhubungan dengan ketepatan dan kelengkapan informasi yang secara validitasnya selaras dengan nilai bisnis.
5. Ketersediaan : berhubungan dengan ada tidaknya informasi yang dibutuhkan

oleh proses bisnis saat ini dan di masa yang akan datang.

6. Kepatuhan : berhadapan dengan pemenuhan terhadap hukum, peraturan dan persetujuan terhadap kontrak dimana proses bisnis.
7. Keakuratan : berhubungan dengan kecocokan informasi yang dibutuhkan oleh manajemen untuk mengoperasikan entitas dan mengatur pelatihan keuangan dan tanggung jawab kepemimpinan.

CobIT juga memungkinkan untuk mengembangkan peraturan - peraturan dan penerapan pengendalian IT yang baik pada keseluruhan perusahaan. CobIT juga bermanfaat dalam memaksimalkan investasi IT serta membantu dalam pengambilan keputusan investasi IT sehingga sistem kendali intern dan proses bisnis perusahaan berjalan baik.

2.7.1 Kerangka Kerja CobIT

Menurut Gondodiyoto (2007, p279) kerangka kerja CobIT terdiri atas beberapa arahan (guidelines), yakni:

1. Control Objectives

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

1. Plan and Organize (PO)

Domain ini meliputi pembahasan strategi investasi TI yang dapat memberikan kontribusi terbaik dalam penerapan tujuan bisnis. Untuk

pencapaiannya, perlu adanya perencanaan, komunikasi dan pengaturan untuk mencapai sasaran bisnis.

Plan and Organize terdiri dari :

- a. PO1 *Define a Strategic IT Plan* (mendefinisikan strategi perencanaan TI).
- b. PO2 *Define the Information Architecture* (mendefinisikan arsitektur informasi).
- c. PO3 *Determine Technological Direction* (menetapkan arah teknologi).
- d. PO4 *Define the IT process, organization and relationship*(mendefinisikan proses, organisasi, dan hubungan TI).
- e. PO5 *Manage the IT investment* (mengatur investasi TI).
- f. PO6 *Communicate Management Aims and Direction* (mengkomunikasikan sasaran dan arah manajemen).
- g. PO7 *Manage IT Human Resources* (mengelola sumber daya manusia TI).
- h. PO8 *Manage Quality* (mengelola kualitas).
- i. PO9 *Assess and Manage IT Risk* (menilai dan mengelola resiko IT)
- j. PO10 *Manage Project* (mengelola proyek).

2. *Acquire and Implement (AI)*

Domain ini meliputi pembahasan tentang bagaimana merealisasikan strategi IT tersebut, solusi perlu untuk diidentifikasi,

dikembangkan atau diperoleh, seperti halnya diimplementasikan dan terintegrasi ke dalam proses bisnis. Sebagai tambahan, perubahan dan pemeliharaan dari sistem yang berjalan dapat diatasi oleh domain untuk memastikan solusi mendapatkan titik temu sasaran bisnis.

Acquire and Implement terdiri dari :

- a. A11 *Identify Automated Solutions* (mengidentifikasi solusi secara otomatis).
- b. A12 *Acquire and Maintain Application* (memperoleh dan merawat aplikasi piranti lunak).
- c. A13 *Acquire and Maintain Technology Infrastructure*(memperoleh dan merawat teknologi infrastruktur).
- d. A14 *Enable operation and Use* (memperbolehkan operasi dan penggunaan).
- e. A15 *Procure IT Resources* (memperoleh sumber daya)
- f. A16 *Manage Changes* (mengelola perubahan).
- g. A17 *install and accredit solutions and changes* (mengukuhkan dan mengakui solusi dan perubahan).

3. *Deliver and Support* (DS)

Domain ini lebih berpusat pada ukuran tentang aspek dukungan TI terhadap kegiatan operasional bisnis.

Deliver and Support terdiri dari :

- a. DS1 *Defines and Manage service Level* (mendefinisikan dan mengelola tingkat layanan)
- b. DS2 *Manage Third-party Services* (mengelola layanan pihak

ketiga).

- c. DS3 *Manage performance and Capacity* (mengelola pelaksanaan dan kapasitas).
- d. DS4 *Ensure Continuous Service* (memastikan layanan berkelanjutan).
- e. DS5 *Ensure Systems Security* (memastikan keamanan sistem).
- f. DS6 *Identify and Allocate Costs* (mengidentifikasi dan mengalokasi biaya).
- g. DS7 *Educate and Train Users* (mendidik dan melatih pengguna).
- h. DS8 *Manage Service Desk and Incidents* (mengelola pelayanan dan peristiwa).
- i. DS9 *Manage the Configuration* (mengelola konfigurasi).
- j. DS10 *Manage Problems* (mengelola masalah)
- k. DS11 *Manage Data* (mengelola data).
- l. DS12 *Manage the Physical Environment* (mengelola lingkungan secara fisik).
- m. DS13 *Manage Operations* (mengelola operasi - operasi).

4. *Monitor and Evaluate* (ME)

Semua proses TI perlu untuk ditaksir secara berkala untuk mengetahui mutu dan tujuan dukungan TI tercapai dengan kebutuhan pengendalian.

Monitor and Evaluate terdiri dari :

- a. ME1 *Monitor and Evaluate IT Performance* (memonitor

dan mengevaluasi kemampuan TI).

b. ME2 *Monitor and Evaluate Internal Control* (memonitor dan mengevaluasi pengendalian intern).

c. ME3 *Ensure Compliance with External Requirements* (memastikan pemenuhan terhadap kebutuhan ekstern).

d. ME4 *Provide IT Governance* (menyediakan kepemimpinan TI).

2. *Audit Guidelines*

Berisi sebanyak 210 tujuan-tujuan pengendalian rinci (*detailed control objectives*) untuk membantu para auditor dalam memberikan *management assurance* dan saran perbaikan.

3. *Management Guidelines*

Berisi arahan, baik secara umum maupun spesifik, mengenai apa saja yang mesti dilakukan, terutama agar dapat menjawab pertanyaan-pertanyaan berikut:

- a. Sejauh mana TI harus bergerak dan apakah biaya TI yang dikeluarkan sesuai dengan manfaat yang dihasilkan ?
- b. Apa saja indikator untuk suatu kinerja yang bagus ?
- c. Apa saja factor atau kondisi yang harus diciptakan agar dapat mencapai sukses (*critical success factor*) ?

- d. Bagaimana dengan perusahaan lainnya, apa yang mereka lakukan ?
- e. Bagaimana anda mengukur keberhasilan dan menilainya ?

2.7.2 *Maturity Model*

Para manajer senior di dalam perseroan atau perusahaan umum semakin diminta untuk memperhatikan bagaimana Teknologi Informasi diatur sebaik mungkin. Oleh karena itu, kasus - kasus bisnis membutuhkan pengembangan untuk peningkatan dan mencapai level yang tepat dari sebuah manajemen dan pengendalian terhadap infrastruktur informasi. Maka dibuatlah suatu skala penilaian yang disebut *Maturity Model*.

Dalam CobIT 4.1. (2007). *Maturity model* adalah suatu cara dalam mengukur sebagaimana baik manajemen proses telah di kembangkan, contohnya seberapa jauh kemampuan perusahaan sebenarnya. Bagaimana sebaiknya pengembangan atau kemampuan menjadi yang utama bergantung pada tujuan IT dan bisnis bisnis yang terkait butuh bantuan *Maturity Model*.

Maturity Model ini digunakan sebagai skala penilaian atau cara mengukur kondisi perkembangan suatu proses manajemen dalam CobIT yang digunakan untuk menentukan pilihan strategi yang digunakan dan melakukan perbandingan dengan standar yang ada, sehingga dapat membantu manajemen dalam mengidentifikasi kinerja yang ingin dicapai dan target perusahaan untuk pengembangan lebih lanjut.

Enam *level* penilaian *Maturity Model* pada CobIT terdiri dari :

1. Level 0 *Non – existent*

Pengelolaan TI masih dalam tahap paling awal, perusahaan belum

mengetahui akan persoalan yang dituju untuk ditangani sehingga setiap proses belum terdefinisi dengan baik.

2. Level 1 *Initial / Ad Hoc*

Walaupun belum ada standar proses yang harus dilakukan, tetapi perusahaan telah menyadari bahwa perlu adanya penanganan mengenai persoalan yang dihadapi berdasarkan kasus - kasus yang muncul. Tetapi secara umum manajemen belum terorganisasi, pengelolaan yang ada belum berjalan dengan baik dan tidak terencana.

3. Level 2 *Repeatable but Intuitive*

Proses telah mengalami perkembangan menuju tahap dimana prosedur yang ada merupakan tanggung jawab individu walaupun belum ada standar prosedur yang diterapkan. Mulai memperhitungkan kelayakan.

4. Level 3 *Defined Process*

Prosedur telah distandarisasi, di dokumentasi dan di komunikasikan melalui pelatihan. Tahap ini memulai mengenal metodologi pengembangan sistem

5. Level 4 *Managed and Measurable*

Pada tahap ini dilakukan pengawasan manajemen dan pengukuran kesesuaian terhadap prosedur, serta tanggap apabila proses tidak bekerja secara efektif. Proses dilakukan dibawah pengembangan secara konstan dan otomatis masih terbatas dan terpisah-pisah.

6. Level 5 *Optimized*

Proses telah mencapai level pelatihan yang baik, berdasarkan hasil pengembangan yang berkelanjutan. TI digunakan sebagai jalan terintegrasi

untuk mengotomatisasi aliran kerja, sebagai alat bantu untuk meningkatkan kualitas dan efektifitas dan membuat perusahaan lebih cepat beradaptasi.

2.8 Diagram UML

2.8.1 Pengertian Diagram UML

Menurut Rama dan Jones (2008,p.79), Diagram aktivitas UML memainkan peran seperti sebuah “peta” dalam memahami proses bisnis dengan menunjukkan urutan aktivitas di dalam proses.

2.8.2 Overview Activity Diagram (OAD)

Menurut Rama, Jones (2008, p.79), OAD menyajikan suatu pandangan tingkat tinggi dari proses bisnis dengan mendokumentasikan kejadian-kejadian penting, urutan kejadian-kejadian ini, dan aliran informasi antar kejadian.

Menurut Rama, Jones (2008,p.85), langkah-langkah membuat *overview activity diagram* yaitu :

Langkah pendahuluan :

Langkah 1 : Membaca uraian narasi dan mengidentifikasi kejadian penting.

Langkah 2 : Membubuhi keterangan pada narasi agar lebih jelas menunjukkan batasan kejadian dan nama-nama kejadian.

Langkah 3 : Menunjukkan agen yang terlibat di dalam proses bisnis dengan menggunakan *swimlanes*.

Langkah 4 : Membuat diagram untuk masing-masing kejadian. Tunjukkan urutan kejadian ini.

Langkah 5 : Menggambarkan dokumen yang dibuat dan digunakan di dalam proses bisnis. Tunjukkan arus informasi dari kejadian ke dokumen, dan sebaliknya.

Langkah 6 : Menggambarkan Tabel (*file*) yang dibuat dan digunakan di dalam proses bisnis. Tunjukkan arus informasi dari kejadian ke table dan sebaliknya.

2.8.3 Detailed Activity Diagram (DAD)

Menurut Rama, Jones (2008, p.80), *Detailed diagram* sama dengan peta dari sebuah kota. Diagram ini menyediakan suatu penyajian yang lebih detil dari aktivitas yang berhubungan dengan satu atau dua kejadian yang ditunjukkan pada *overview diagram*.

Rama , Jones (2008,p.111), symbol-simbol yang digunakan dalam diagram aktivitas adalah :

a. Lingkaran penuh

Lingkaran penuh menunjukkan awal dari proses. Lingkaran ini muncul di dalam *swim lane* agen (di dalam atau di luar organisasi itu) yang memulai proses.

b. Segi Empat Panjang

Segi empat panjang menunjukkan *event*, aktivitas, atau pemicu (*trigger*) yang menyebabkan satu agen dalam organisasi untuk melaksanakan beberapa tindakan selanjutnya.

c. Garis tidak terputus

Garis dengan panah digunakan untuk menunjukkan urutan kejadian.

d. Dokumen

Teks ini menggunakan simbol dokumen untuk menunjukkan dokumen sumber dan laporan.

e. Berlian

Menunjukkan sebuah cabang.

f. Garis putus-putus

Garis putus-putus dengan panah digunakan untuk menunjukkan aliran informasi antar kejadian.

g. Tabel

Simbol tabel menunjukkan data mungkin dibaca atau dicatat di dalam *file* komputer selama kejadian bisnis.

h. Mata banteng

Simbol mata banteng menunjukkan akhir dari proses.