



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB II

LANDASAN TEORI

2.1 Audit Sistem Informasi

2.1.1 Audit

Menurut ASOBAC (*A Statement of Basic Auditing Concepts*), audit merupakan sebuah proses sistematis untuk mendapatkan dan mengevaluasi bukti kejadian ekonomi secara obyektif mengenai kebijakan serta aktivitas ekonomi untuk menentukan tingkat kecocokan/kesesuaian antara pernyataan dengan kriteria yang telah ditetapkan dan menyampaikan hasilnya kepada pihak yang berkepentingan. Berikut pengertian audit menurut beberapa ahli:

Menurut Mulyadi (2002), suatu proses sistematis 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.

Menurut Arens, dkk (2011), audit adalah akumulasi dan evaluasi tentang informasi untuk menentukan dan melaporkan tingkat kesesuaian antara informasi dan kriteria yang telah ditetapkan. Audit harus dilakukan oleh seorang yang kompeten dan independen.

Menurut Sukrisno (1996), audit merupakan suatu pemeriksaan terhadap laporan yang sudah disusun oleh manajemen serta catatan pembukuan disertai bukti-bukti pendukung yang dilakukan secara sistematis dan kritis oleh pihak yang independen, yang bertujuan bisa memberikan suatu pendapat atas kewajaran laporan keuangan.

Dapat disimpulkan dari pengertian di atas bahwa audit adalah proses untuk mengakumulasi dan mengevaluasi kegiatan ekonomi, lalu memastikan bahwa sudah sesuai dengan kriteria yang sudah ditetapkan di awal. Audit dilakukan oleh orang yang kompeten dan independen, karena dalam melakukan audit harus konsisten dalam memberikan tenaganya dalam bekerja dan spesifik dalam bekerja serta independen dalam melakukan pekerjaannya.

2.1.2 Sistem Informasi

Istilah sistem informasi yang sering digunakan merujuk kepada interaksi antara orang, proses algoritma, data dan teknologi yang berarti penggunaan teknologi informasi dan komunikasi tidak hanya pada perusahaan atau organisasi. Tetapi juga cara orang berinteraksi dengan teknologi untuk menunjang proses bisnisnya (*Software Engineering Institute*).

Menurut Kertahadi (dalam Fatta, 2007), sistem informasi adalah alat untuk menyajikan informasi sedemikian rupa sehingga bermanfaat bagi penerimanya. Tujuannya adalah untuk memberikan informasi dalam

perencanaan, memulai, pengorganisasian, operasional sebuah perusahaan yang melayani sinergi organisasi dalam proses mengendalikan pengambilan keputusan.

Menurut Sutabri (2005), sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi organisasi yang bersifat manajerial dalam kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan-laporan yang dilakukan.

Menurut McLeod (2001), sistem informasi merupakan sistem yang mempunyai kemampuan untuk mengumpulkan informasi dari semua sumber dan menggunakan berbagai media untuk menampilkan informasi.

Menurut Davis (1991), sistem informasi adalah suatu sistem yang menerima masukan data dan instruksi, mengolah data tersebut sesuai dengan instruksi dan mengeluarkan hasilnya.

Dapat disimpulkan pengertian sistem informasi di atas, bahwa sistem informasi adalah sistem yang digunakan oleh sebuah organisasi dan perusahaan untuk kebutuhan pengolahan data dan transaksi yang terjadi dan dikumpulkan agar menjadi satu sumber dan dapat dijadikan untuk informasi sebagai hasilnya, serta dapat membantu dalam mengambil keputusan bagi perusahaan atau organisasi.

Fungsi dari sistem informasi sendiri adalah untuk memperbaiki pengembangan dan pemeliharaan sistem agar kualitasnya tetap terjaga,

melihat dari risiko-risiko yang dapat terjadi di dalam proses bisnis suatu organisasi atau perusahaan. Sistem informasi juga membantu pihak organisasi atau perusahaan untuk mengambil keputusan jika terjadi masalah dalam pengoperasiannya.

2.1.3 Audit Sistem Informasi

Audit sistem informasi adalah proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumber daya secara efisien (Weber, 1999).

Audit sistem informasi adalah proses mengumpulkan dan mengevaluasi bukti untuk menentukan derajat kesesuaian antara informasi dan kriteria yang ditetapkan. Maka dari itu, dalam pelaksanaan evaluasi dilakukan mengacu kepada sejumlah kriteria untuk menentukan derajat kinerja yang telah dicapai (Arens ,dkk, 2002).

Audit sistem informasi merupakan suatu proses evaluasi untuk mengetahui bagaimana tingkat kesesuaian antara aplikasi sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah suatu sistem informasi telah didesain dan diimplementasikan dengan baik dan ekonomis, serta memiliki mekanisme pengamanan aset yang memadai, menjamin integritas data (Gondodiyoto, 2003).

Audit sistem informasi merupakan proses pengumpulan dan pengevaluasian bukti untuk menentukan apakah sistem informasi dapat melindungi aset dan teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan pada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif dan efisien (Sarno, 2009).

Dengan demikian, audit sistem informasi merupakan proses melakukan evaluasi dan pengumpulan bukti terhadap sistem informasi yang ada di sebuah perusahaan, apakah sudah berjalan dengan seharusnya dan memiliki pengamanan yang baik terhadap data-datanya.

2.2 Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Weber (1999) dibagi menjadi 4 tahap, yaitu sebagai berikut:

1. Pengamanan Aset

Aset yang dimaksudkan seperti informasi perusahaan, *hardware*, *software*, sumber daya manusia, dan dokumen-dokumen perusahaan harus dijaga oleh sistem pengendalian internal agar tidak terjadi penyalahgunaan aset perusahaan. Oleh karena itu, pengamanan aset merupakan hal penting untuk dipenuhi oleh organisasi atau perusahaan.

Dalam PT. Assalam Madani Wisata Barokah, aset yang perlu dijaga keamanannya adalah data dari pelanggan mereka. Data

pelanggan berisi mengenai informasi penting pelanggan, jika data sampai bocor maka pelanggan akan merasa tidak aman dan merasa tidak bisa mempercayakan data mereka pada perusahaan.

2. Menjaga Integritas Data

Integritas data merupakan salah satu konsep dasar sistem informasi. Data memiliki atribut penting, yaitu kelengkapan, kebenaran, dan keakuratan. Jika integritas data tidak terpelihara dengan baik, maka organisasi atau perusahaan tidak akan menghasilkan dan memiliki laporan yang benar bahkan dapat merugi.

Dalam PT. Assalam Madani Wisata Barokah, data yang diberikan kepada pelanggan harus benar dan akurat mengingat perusahaan ini bergerak dibidang jasa maka data yang diberikan pelanggan harus benar. Data yang benar untuk menjaga jika ada suatu hal yang tidak baik terjadi maka dapat ditangani dengan mudah, misalnya jemaah hilang dari rombongan dapat dengan mudah dihubungi.

3. Efektifitas Sistem

Efektifitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan. Suatu sistem informasi dapat dikatakan efektif bila sistem informasi telah sesuai dengan kebutuhan *user*.

Dalam PT. Assalam Madani Wisata Barokah sistem yang digunakan hanya untuk internal jadi hanya karyawan saja yang menggunakannya. Untuk menunjang proses bisnis agar berjalan dengan lancar, maka sistem informasi harus sesuai dengan kebutuhan user dan selalu melakukan pengembangan dan perbaikan sesuai dengan kebutuhan.

4. Efisiensi Sistem

Ketika komputer sudah tidak memiliki kapasitas yang memadai maka efisiensi menjadi penting dan harus melakukan evaluasi terhadap sistem, apakah sistem sudah benar-benar memadai atau belum. Sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya informasi yang minim.

Dalam PT. Assalam Madani Wisata Barokah membutuhkan banyak tempat didalam sistem untuk menyimpan data pelanggan mereka.

5. Ekonomis

Ekonomis di sini mencerminkan kalkulasi untuk rugi secara ekonomi yang lebih bersifat kuantifikasi nilai moneter (uang). Efisiensi berarti sumber daya minimum untuk mencapai hasil maksimal, sedangkan ekonomis lebih bersifat pertimbangan ekonomi.

Dalam PT. Assalam Madani Wisata Barokah dengan adanya teknologi informasi yang memadai dapat meminimalisir pengeluaran bagi mereka dan tidak memerlukan sumber daya yang banyak.

a. Kerangka Audit

i. COSO (*Committee of Sponsoring Organizations of the Treadway Commission*)

COSO merupakan sebuah inisiatif bersama dari lima organisasi sektor swasta yang terdaftar dan didedikasikan untuk menyediakan kepemimpinan pemikiran melalui pengembangan kerangka kerja dan pedoman risiko manajemen perusahaan, pengendalian internal dan penipuan pencegahan (COSO, 1 April 2016).

COSO memiliki tujuan untuk memberikan kepemimpinan pemikiran melalui pengembangan kerangka kerja yang komprehensif dan bimbingan pada risiko manajemen perusahaan, pengendalian internal dan penipuan pencegahan yang dirancang untuk

meningkatkan kinerja organisasi tata kelola dan untuk mengurangi tingkat kecurangan data organisasi (COSO, 1 April 2016).

ii. **ITIL (*Information Technology Infrastructure Library*)**

ITIL adalah serangkaian dokumen yang digunakan untuk membantu pelaksanaan kerangka siklus hidup untuk ITSM. Kerangka yang disesuaikan ini mendefinisikan bagaimana layanan manajemen diterapkan dalam sebuah organisasi (ITIL, 1 April 2016).

ITIL memberikan deskripsi detail tentang beberapa praktik TI penting dengan daftar cek, tugas, serta prosedur yang menyeluruh yang dapat disesuaikan dengan segala jenis organisasi TI. ITIL memiliki siklus layanan yang diterbitkan oleh OGC (*Office of Government Commerce*) yang terdiri dari 5 bagian sebagai berikut:

1. ***Service Strategy***

Memberikan panduan kepada orang yang melakukan implementasi ITSM untuk memandang konsep dari ITSM tidak hanya sekedar sebagai kemampuan organisasi dalam memberikan, mengelola dan mengoperasikan layanan TI, tetapi juga sebagai aset perusahaan. Panduan ini dibentuk menjadi prinsip-prinsip dasar dari konsep ITSM, acuan dan proses inti yang beroperasi di keseluruhan tahapan ITIL *Service Lifecycle*.

2. *Service Design*

Agar layanan TI bermanfaat maka sebelum digunakan harus didesain terlebih dahulu sesuai dengan tujuan pelaku bisnis.

Service design memberikan panduan kepada organisasi TI untuk mendesain secara sistematis dan mudah digunakan saat nanti diimplementasikan.

3. *Service Transition*

Menyediakan panduan yang bersifat mengembangkan hasil desain layanan TI, dan kemampuan untuk merubahnya dalam proses yang terjadi di organisasi atau perusahaan.

4. *Service Operation*

Mencakup semua kegiatan operasional harian pengelolaan layanan-layanan TI, yang di dalamnya terdapat panduan bagaimana mengelola layanan TI agar efektif dan efisien untuk menjamin tingkat kinerja yang telah dijanjikan dengan *user*.

5. *Continual Service Improvement (CSI)*

Memberikan panduan untuk menyusun serta memelihara kualitas layanan TI, mulai dari proses desain, transisi dan pengoperasiannya.

2.3 COBIT (*Control Objective for Information & Related Technology*)

2.3.1 Definisi COBIT

COBIT adalah sekumpulan dokumentasi *best practice* untuk *IT Governance* yang dapat membantu auditor, *user*, dan manajemen untuk menjembatani antara risiko bisnis, kebutuhan kontrol dan masalah-masalah teknis TI (Sasongko, 2009).

COBIT merupakan pemberian layanan kerangka kerja secara komprehensif untuk membantu pemerintah dan manajemen TI dalam sebuah perusahaan mencapai tujuan yang diharapkan (ISACA, 2016).

2.3.2 Sejarah COBIT

COBIT merupakan *framework* yang diterbitkan oleh ISACA (*Information System Audit and Control Association*) pertama kali pada tahun 1996, yang kemudian pada tahun 1998 diterbitkan COBIT edisi kedua. Pada tahun 2000, COBIT 3.0 dirilis dan pada tahun 2005, COBIT 4.0 dirilis. Kemudian COBIT 4.1 dirilis pada tahun 2007 dan yang terbaru adalah COBIT 5.0 yang dirilis pada tahun 2012.

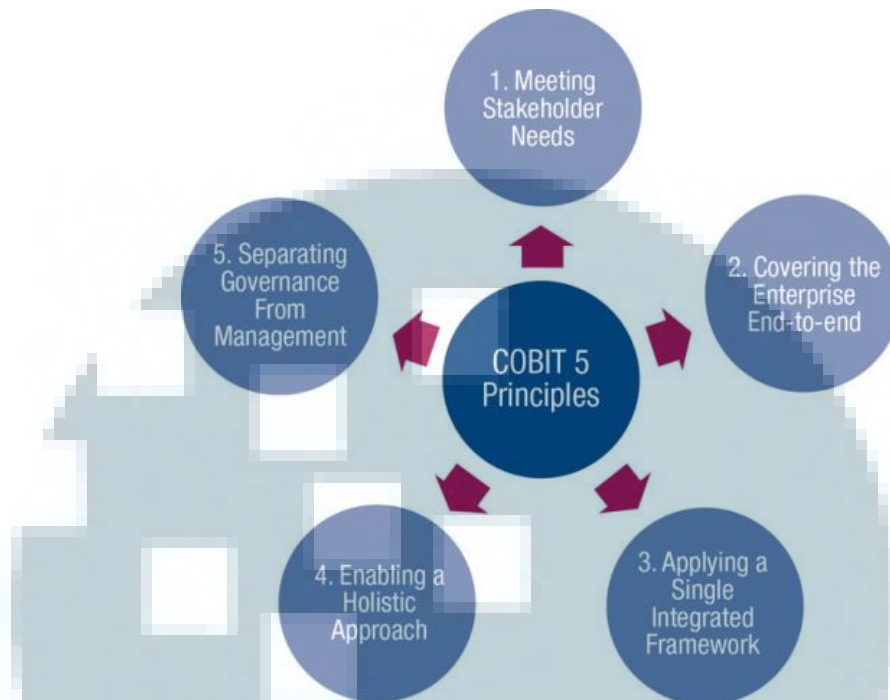
2.3.3 COBIT 5.0

A. COBIT 5.0 *Enabler*

Enabler adalah segala sesuatu yang dapat membantu pencapaian tujuan dari perusahaan. COBIT 5.0 mendefinisikan 7 kategori enabler, antara lain:

1. Prinsip, kebijakan dan kerangka kerja yang menerjemahkan perilaku yang diinginkan ke dalam panduan yang praktis untuk manajemen.
2. Proses, menggambarkan praktik dan kegiatan untuk mencapai tujuan tertentu.
3. Struktur organisasi, sebagai kunci entitas pengambilan keputusan dalam suatu perusahaan.
4. Budaya, etika dan perilaku, individu dan perusahaan.
5. Informasi yang menyebar di seluruh organisasi dan mencakup semua informasi yang dihasilkan dan digunakan oleh perusahaan. Informasi diperlukan untuk menjaga jalannya organisasi.
6. Layanan, infrastruktur dan aplikasi. Menyediakan perusahaan dengan pengolahan informasi dan layanan teknologi.
7. Orang, keahlian dan kompetensi. Diperlukan orang-orang yang dapat menyelesaikan semua kegiatan dan membuat keputusan yang benar mengambil tindakan korektif.

Penjelasan 5 prinsip COBIT 5.0 dapat dilihat pada Gambar 2.1.



Gambar 2.1 Prinsip COBIT 5.0

(Sumber: www.isaca.org)

a. Meeting stakeholder needs

Kebutuhan *stakeholder* diterjemahkan ke dalam *Goals Cascade* menjadi tujuan yang lebih spesifik, dapat ditindak lanjuti dan disesuaikan, dalam konteks, tujuan perusahaan, tujuan yang terkait (*IT-related goal*), tujuan yang akan dicapai *enabler*. Sistem tata kelola juga harus mempertimbangkan seluruh *stakeholder* ketika membuat keputusan mengenai penilaian manfaat, *resource* dan risiko.

b. Covering Enterprise End-to-End

Bermanfaat untuk mengintegrasikan tata kelola TI perusahaan ke dalam tata kelola perusahaan. Sistem tata kelola TI yang diusung COBIT 5.0 dapat menyatu dengan

sistem tata kelola perusahaan dengan lancar. Prinsip kedua ini juga meliputi fungsi dan proses yang dibutuhkan untuk mengukur dan mengelola TI perusahaan dimanapun informasi diproses. Dalam perusahaan, COBIT 5.0 menangani semua layanan TI internal maupun eksternal, dan juga proses bisnis internal dan eksternal.

c. *Applying a Single Integrated Framework*

Prinsip ini menyatukan semua pengetahuan yang sebelumnya tersebar dalam berbagai *framework* ISACA (COBIT, VAL IT, Risk IT, BMIS, ITAF), sehingga perusahaan mampu menggunakan COBIT 5.0 sebagai *framework* tata kelola umum dan *integrator*.

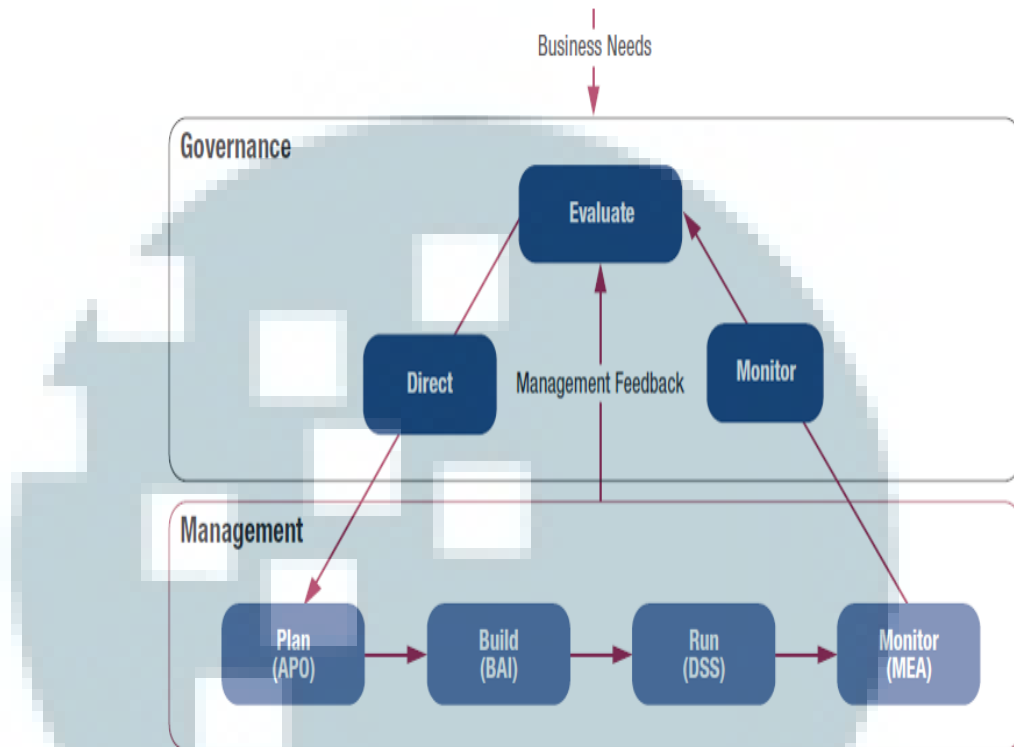
d. *Enabling a Holistic Approach*

COBIT 5.0 memandang bahwa setiap *enabler* saling mempengaruhi satu sama lain dan menentukan apakah penerapan COBIT 5.0 akan berhasil.

e. *Separating Governance From Management*

COBIT 5.0 membuat perbedaan yang cukup jelas antara tata kelola dan manajemen. Kedua hal tersebut mencakup berbagai kegiatan yang berbeda, memerlukan struktur organisasi yang berbeda dan melayani untuk tujuan yang berbeda pula.

2.3.4 Proses Model COBIT 5.0

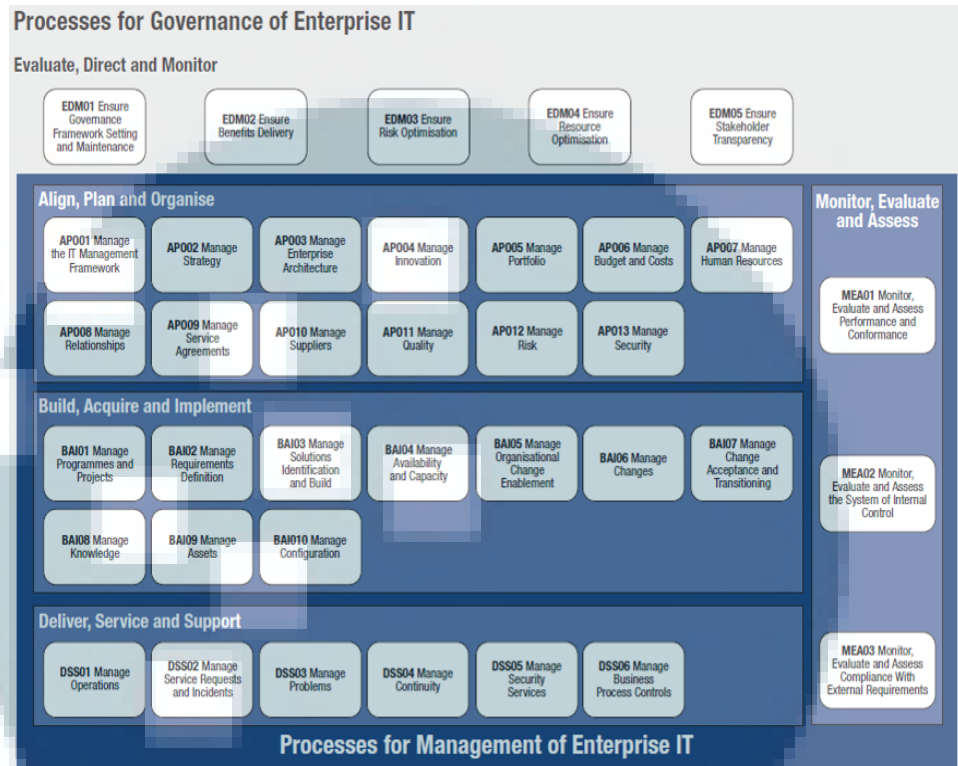


Gambar 2.2 Proses Model COBIT 5.0
(Sumber: www.isaca.org)

Pada gambar 2.2 dijelaskan bahwa COBIT 5.0 membagi proses tata kelola dan manajemen TI perusahaan menjadi dua domain proses utama, antara lain:

1. *IT Governance*, memuat lima proses tata kelola, di mana akan ditentukan praktik-praktik dalam setiap proses *Evaluate*, *Direct*, and *Monitor* (EDM).
2. Manajemen, memuat empat domain, sejajar dengan area tanggung jawab dari *Plan*, *Build*, *Run* and *Monitor* (PBRM), dan menyediakan ruang lingkup TI yang menyeluruh dari ujung ke ujung.

2.3.5 Proses Referensi Model COBIT 5.0



Gambar 2.3 Proses Referensi Model COBIT 5.0

(Sumber: www.isaca.org)

Pada gambar 2.3 menjelaskan lengkap 37 set dari tata kelola dan manajemen TI dalam proses COBIT 5.0.

a. Penjelasan Proses

COBIT 5.0 proses referensi model adalah subdivisi *IT Governance* dan proses manajemen dari *enterprise IT* ke dalam dua area utama dari aktifitas, 2 proses itu sebagai berikut:

1. *Governance* (tata kelola)

Terdiri dari lima proses tata kelola, yang mana setiap prosesnya praktik EDM (*Evaluate, Direct, Monitor*) yang

digunakan. Penjelasan proses pada praktik EDM yang digunakan sebagai berikut:

- a. *Evalute* - Mengidentifikasi dan menyetujui tujuan yang akan dicapai oleh organisasi.
- b. *Direct* - Menentukan prioritas berdasarkan pengambilan keputusan.
- c. *Monitor* - Pengawasan kinerja berdasarkan kepatuhan terhadap tujuan organisasi.

2. *Management*

Ada empat proses yang menjadi tanggung jawab PBRM dan tersedia *end-to-end* dari TI. Penjelasan proses pada praktik PBRM (*Plan, Build, Run, Monitor*) yang digunakan sebagai berikut:

- a. Memastikan semua aktivitas dilakukan dan diawasi.
- b. Memastikan semua aktivitas selaras dengan apa yang diarahkan berdasarkan fungsi tata kelola.

b. Penjelasan Tahapan Penggunaan COBIT 5.0

Dalam penggunaan *framework* COBIT 5.0, tahap pertama adalah dengan melakukan proses pada tata kelola TI dengan menggunakan modul EDM. Penjelasan proses pada EDM sebagai berikut:

1. *Evalute, Direct, Monitor*

- a. EDM01 - Memastikan tata pengaturan kerangka dan pemeliharaan.

- b. EDM02 - Memastikan manfaat pengiriman.
- c. EDM03 - Memastikan optimasi pengendalian risiko.
- d. EDM04 - Memastikan optimisasi sumber daya.
- e. EDM05 - Memastikan *stakeholder* transparansi.

Proses yang dilakukan pada manajemen adalah dengan menggunakan PBRM (*Plan, Build, Run and Monitor*) penjelasannya sebagai berikut:

1. *Align, Plan, and Organize (APO) - Plan*

- a. APO01 - Mengelola Kerangka Kerja Manajemen TI.
- b. APO02 - Mengelola Strategi.
- c. APO03 - Mengelola Arsitektur Perusahaan.
- d. APO04 - Mengelola Inovasi.
- e. APO05 - Mengelola Portofolio.
- f. APO06 - Mengelola Anggaran dan Biaya.
- g. APO07 - Mengelola Sumber Daya.
- h. APO08 - Mengelola Hubungan.
- i. APO09 - Mengelola Perjanjian.
- j. APO10 - Mengelola Pemasok.
- k. APO11 - Mengelola Kualitas.
- l. APO12 - Mengelola Risiko.
- m. APO13 - Mengelola Keamanan.

2. *Build, Acquare, and Implement (BAI) - Build*

- a. BAI01 - Mengelola Program dan Proyek.

- b. BAI02 - Mengelola Definisi Persyaratan.
 - c. BAI03 - Mengelola Solusi Identifikasi dan Pembangunan.
 - d. BAI04 - Mengelola Ketersediaan dan Kemampuan.
 - e. BAI05 - Mengelola Perubahan Organisasi PEMBERDAYAAN.
 - f. BAI06 - Mengelola Perubahan.
 - g. BAI07 - Mengelola Perubahan Penerimaan dan Transisi.
 - h. BAI08 - Mengelola Pengetahuan.
 - i. BAI09 - Mengelola Aset.
 - j. BAI10 - Mengelola Konfigurasi.
3. *Deliver, Service, and Support (DSS) - Run*
- a. DSS01 - Mengelola Operasi.
 - b. DSS02 - Mengelola Permintaan Layanan dan Peristiwa.
 - c. DSS03 - Mengelola Masalah.
 - d. DSS04 - Mengelola Kontinuitas.
 - e. DSS05 - Mengelola Pelayanan Keamanan.
 - f. DSS06 - Mengelola Kontrol Proses Bisnis.
4. *Monitor, Evaluate and Assess (MEA) - Monitor*
- a. MEA01 - Mengamati, Evaluasi dan Menilai Kinerja dan Kesesuaian.

b. MEA02 - Mengamati, Evaluasi, dan Menilai Sistem dari *Internal Control*.

c. MEA03 - Evaluasi dan Menilai Pemenuhan Persyaratan Eksternal.

c. **Capability Level**

1. Definisi *Capability Level*

Capability level adalah sebuah model untuk menggambarkan bagaimana setiap proses berjalan dalam sebuah organisasi atau perusahaan. Setiap organisasi atau perusahaan tentu memiliki lebih dari satu proses. Dalam setiap proses, tentu organisasi atau perusahaan memiliki satu atau dua proses penting bagi mereka yang terletak pada level 4 atau 5 (CMMI, 2014). Berikut adalah proses yang ada pada *capability level*:

Tabel 2.1 Proses Pada *Capability Level*

Level 0 Incomplete Process
Proses ini tidak dilaksanakan atau gagal untuk mencapai tujuannya.
Level 1 Performed Process
Proses dilaksanakan dan mencapai tujuannya.
Level 2 Managed Process
Proses ini dikelola dimana produk kerja tepat didirikan, dikendalikan dan dipelihara.
Level 3 Established Process
Proses didefinisikan yang digunakan berdasarkan standar proses.

Level 4 Predictable Process
Proses ditetapkan dalam batas yang ditentukan.
Level 5 Optimizing Process
Proses terus ditingkatkan untuk memenuhi tujuan bisnis saat ini dan proyeksi yang relevan.

2. Perhitungan *Capability Level*

Cara menghitung *capability level* dilakukan dengan menggunakan rumus rata-rata sebagai berikut:

$$Capability\ level = \frac{(0*y_0) + (1*y_1) + \dots + (5*y_5)}{z}$$

Rumus 2.1 Rumus *Capability Level*

Keterangan:

y-n (y0...y5) = jumlah proses yang berada di level n

z = jumlah proses yang dievaluasi

Dapat dilihat pada rumus 2.1 adalah rumus untuk menghitung *capability level* dimana dari proses COBIT 5.0 yang digunakan, setiap subproses dari masing-masing proses dijumlahkan hasilnya lalu dibagi dengan jumlah subproses dari masing-masing proses COBIT 5.0. Maka, akan mendapatkan hasil rata-rata untuk masing-masing proses pada COBIT 5.0.