BAB II

TELAAH LITERATUR

Dalam penulisan penelitian ini, ada beberapa pengertian yang berhubungan dengan audit sistem informasi yang diajukan, karena tanpa pegangan teori yang jelas akan menyebabkan informasi yang disajikan tidak sesuai dengan yang diharapkan.

2.1 Tinjauan Pustaka

2.1.1 Pengertian *Auditing*

Auditing merupakan asersi tentang kewajaran penyajian laporan keuangan. Konrath (2002:5) merumuskan definisi umum dari *auditing*,

> "*Auditing* adalah suatu proses sistematis untuk mendapatkan dan mengevaluasi bukti mengenai asersi tentang kegiatan-kegiatan dan kejadian-kejadian ekonomi untuk menyakinkan tingkat keterkaitan antara asersi tersebut dan kriteria yang telah ditetapkan dan mengkomunikasikan hasilnya kepada pihak-pihak yang berkepentingan."

Arens (2010) menyatakan *auditing* adalah,

> "*Auditing* merupakan suatu akumulasi dan evaluasi dari temuan yang mencerminkan informasi yang menjelaskan dan melaporkan tingkat korespondensi antara informasi dan kriteria. Audit juga dilakukan oleh orang yang berkompeten dan independen.

Whittington, et al (2012) menyatakan bahwa *auditing* yaitu,

> "*Statement* keuangan bahwa auditor mencari bukti dan membuat suatu penjaminan tingkat tinggi yang menyatakan bahwa *statement* keuangan yang dibuat sudah memenuhi prinsip akuntansi termasuk didalamnya suatu proses pencarian dan verifikasi *record* dan mencari temuan-temuan berdasarkan *statement* keuangan dan temuan yang

dihasilkan dibuat suatu laporan yang merupakan opini auditor bahwa *statement* telah memenuhi prinsip akuntansi".

Seputra (2013), definisi *auditing* secara umum adalah:

> "Proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan oleh seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi yang dimaksudkan dengan kriteria-kriteria yang telah ditetapkan".

Mulyadi (2002), definisi *auditing* 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".

Dari beberapa definisi *auditing* di atas, dapat dilihat bahwa *auditing* setidaknya memiliki komponen penting dalam pengertiannya, antara lain:

1. Proses yang sistematis, *auditing* adalah evaluasi dari bukti mengenai asersi tentang kegiatan-kegiatan dan kejadian-kejadian ekonomi untuk menyakinkan tingkat keterkaitan antara asersi tersebut.
2. Temuan-temuan yang dievaluasi dapat menghasilkan informasi-informasi yang dapat menjelaskan dan melaporkan tingkat korespondensi antara informasi dan kriteria.
3. Proses pencarian dan verifikasi *record* dan mencari temuan-temuan berdasarkan *statement* keuangan harus memenuhi prinsip akuntansi.
4. Audit harus dilakukan oleh orang berkompeten dan independen, arti dari yang berkompeten adalah seorang auditor harus benar-benar menguasi

bidangnya sehingga tugas-tugasnya dapat dilaksnaakan dengan baik serta mengambil kesimpulan yang tepat atas pemeriksaan yang telah dilakukan. Sedangkan independen merupakan sikap mental yang harus dimiliki oleh seorang auditor agar dapat menjadi auditor handal.

5. Laporan adalah proses akhir dari tahapan pemeriksaan. Di dalam laporan tersebut terdapat hasil dari temuan ataupun informasi yang akan disampaikan kepada pihak-pihak yang berkepentingan.

Kesimpulan dari beberapa definisi mengenai *auditing* serta komponen-komponen penting yang telah dijabarkan bahwa *auditing* adalah suatu pemeriksaan yang dilakukan secara detail, sistematis oleh pihak yang kompeten serta independen terhadap laporan keuangan yang telah disusun oleh pihak manajemen beserta semua unsur yang ada dalam prinsip akuntansi dengan tujuan untuk dapat memberikan opini tentang kewajaran laporan keuangan tersebut berdasarkan prinsip akuntansi.

2.1.2 Pengertian Sistem

Menurut McLeod (2004: 9), "Sistem adalah sekelompok elemen-elemen yang terintegrasi dengan maksud yang sama untuk mencapai suatu tujuan."

Menurut Romney dan Steinbart (2004: 4), "Sistem adalah satu dari dua atau lebih komponen-komponen yang saling berinteraksi untuk mencapai suatu tujuan."

Menurut O'Brien (2005: 8), "Sistem merupakan sekumpulan komponen-komponen yang saling berhubungan dan bekerja sama untuk mencapai tujuan

bersama, dengan menerima masukan dan menghasilkan pengeluaran melalui proses tranformasi yang terorganisir."

Jadi, dapat disimpulkan bahwa sistem merupakan sekelompok unsur yang erat hubungannya satu dengan yang lain, yang berfungsi bersama-sama untuk mencapai tujuan tertentu.

2.1.3 Pengertian Informasi

Menurut McLeod (2004: 12), "Informasi adalah data yang telah diproses, atau data yang memiliki arti."

Menurut Romney dan Steinbart (2006: 5), "Informasi adalah data yang telah diatur dan diproses untuk memberikan arti kepada pengguna."

Menurut O'Brien (2005: 15), "Informasi adalah data yang telah diubah ke dalam sebuah bentuk yang mempunyai arti dan berguna bagi pemakai tertentu atau khusus.

Dari definisi tersebut di atas dapat diambil kesimpulan bahwa informasi merupakan data yang telah diklasifikasikan atau diolah atau diinterpretasikan untuk digunakan dalam proses pengambilan keputusan.

2.1.4 Pengertian Sistem Informasi

Beberapa pengertian mengenai sistem informasi yang peneliti pegang adalah:

- Gondodiyoto (2007: 112) mendefinisikan sistem informasi merupakan sebagai kumpulan elemen-elemen dan jaringan prosedur

yang saling berkaitan secara terpadu, terintegrasi dalam suatu hubungan hirarkis tertentu, serta bertujuan untuk mengolah data menjadi informasi.

- Hall (2011: 7) mendefinisikan sistem informasi adalah sebuah rangkaian prosedur formal dimana data dikelompokkan, diproses menjadi informasi, dan didistribusikan kepada pemakai.
- Bower (1985: 5) mendefiniskan sistem informasi adalah suatu cara yang sudah tertentu untuk menyediakan informasi yang dibutuhkan oleh organisasi untuk beroperasi dengan cara yang sukses dan untuk organisasi bisnis dengan cara yang menguntungkan.

Kesimpulan yang dapat diambil adalah sistem informasi merupakan suatu sistem dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi operasi organisasi yang bersifat manajerial dengan kegiatan dari suatu organisasi untuk dapat menyediakan laporan-laporan yang diperlukan oleh pihak luar tertentu.

2.1.5 Pengertian Audit Sistem Informasi

Berikut ini merupakan pengertian audit sistem informasi menurut beberapa ahli:

- Basalamah (2003),

> "Audit sistem informasi merupakan suatu proses pengumpulan dan penilaian bukti untuk menentukan apakah suatu sistem komputer melindungi aktiva, mempertahankan integritas data, mencapai tujuan organisasi secara efektif, dan menggunakan sumber daya secara efisien."

- Gondodiyoto (2007),

  "Audit sistem informasi merupakan suatu pengevaluasian untuk mengetahui bagaimana tingkat kesesuaian antara aplikasi sistem informasi dengan prosedur yang telah ditetapkan dan mengetahui apakah suatu sistem informasi telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis yang memiliki mekanisme pengamanan aset yang memandai, serta menjamin integritas data yang memadai."

- Hall (2011) berpendapat bahwa,

  "Audit sistem informasi berfokus pada aspek organisasi sistem informasi berbasis komputer. Audit sistem informasi ini meliputi penilaian terhadap pelaksanaan, operasi, dan pengendalian sumber daya komputer yang tepat. Karena sebagian besar dari sistem informasi mempergunakan teknologi informasi, audit sistem informasi biasanya merupakan komponen yang signifikan dari semua audit eksternal (*financial*) dan audit internal."

Dari pengertian-pengertian para ahli mengenai Audit Sistem Informasi dapat disimpulkan menjadi, proses pengumpulan dan pengevaluasian bukti-bukti untuk membuktikan apakah suatu sistem komputerisasi telah menetapkan dan menerapkan sistem pengendalian intern yang memadai, semua aktiva dilindungi dengan baik atau tidak salah digunakan serta terjamin integritas data, keandalan serta efektifitas dan efisiensi penyelenggaraan sistem informasi berbasis komputer. Audit sistem informasi juga merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan *Behavioral Science*.

2.1.6 Tipe-tipe Audit

Tipe-tipe audit menurut Basalamah (2003) ditemukan beberapa tipe audit. Basalamah (2003) menyatakan bahwa beberapa penulis menyebutkan jumlah jenis

audit yang berbeda. Sebagian menyatakan tiga jenis, sedangkan sebagian menyatakan empat jenis. Berapapun jumlah jenisnya, secara keseluruhan tipe-tipe audit adalah sebagai berikut: (Basalamah, 2003)

- Audit Finansial *(financial audit*) atau disebut juga audit ekstern (*external audit*) atau audit atas laporan keuangan (*financial statement audit* atau *financial report audit*). Audit ini dilakukan terhadap catatan-catatan dan sistem informasi suatu organisasi untuk menilai kewajaran laporan keuangan organisasi tersebut.
- Audit Operasional (*operational audit*) atau disebut juga audit kinerja (*performance audit*) atau audit manajemen (*management audit*), yaitu suatu ulasan atas salah satu bagian dari prosedur-prosedur dan metode-metode operasi suatu organisasi dengan tujuan untuk memberikan rekomendasi mengenai kehematan dan efisiensi penggunaan sumber daya, efektivitas pencapaian sasaran bisnis dan ketaatan terhadap kebijakan-kebijakan perusahaan.
- Audit Internal (*internal audit*), yaitu suatu fungsi penilai yang independen yang ditetapkan dalam suatu organisasi untuk menguji dan mengevaluasi aktivitasnya sebagai pelayanan kepada organisasi tersebut. Tujuannya adalah untuk membantu para anggota organisasi tersebut dalam menjalankan kewajiban mereka secara efektif. Pada akhirnya audit internal memberikan pelayanan kepada mereka dalam bentuk analisis, penilaian, rekomendasi, konseling, dan informasi yang berkaitan dengan aktivitas-aktivias yang dievaluasi.

- *Compliance Audit*, yaitu suatu jenis audit yang bertujuan untuk menentukan apakah auditan mengikuti prosedur-prosedur, hukum atau peraturan-peraturan tertentu yang ditetapkan oleh otoritas yang lebih tinggi, dimana otoritas di sini dapat dalam bentuk kontroler perusahaan, pemerintah (peraturan perundang-undangan), mitra perusahaan dalam pelaksanaan kontrak, dan sebagainya.
- *General Audit*, adalah dari suatu laporan yang dilakukan oleh KAP independen bertujuan dapat memberikan pendapat mengenai kewajaran laporan keuangan secara keseluruhan. *General audit* harus dilakukan sesuai dengan *Standar Professional Akuntan Public* atau ISA atau panduan audit entitas bisnis kecil dan memperhatikan kode etik akuntan Indonesia.
- *Application Audit*, merupakan audit yang dapat berbentuk ulasan sistem aplikasi langsung dalam arena pengguna, audit sistem aplikasi yang sedang dikembangkan, atau audit dari proses sistem pengembangan aplikasi itu sendiri.
- *Audits involving operating system*, kurang peduli dengan audit dari sistem operasi itu sendiri melainkan cara dimana instalasi telah memilih untuk menerapkan opsi sistem operasi.
- *Physical access audits*, audit yang dilakukan dengan cara mengaudit akses fisik kepada aset perusahaan untuk tujuan utama yaitu pengamanan aset perusahaan.

- *Logical access audits*, biasanya akan melibatkan interogasi *file* kontrol sistem komputer agar hak akses yang diberikan sesuai dengan kebutuhan kerja.

2.1.7 Tujuan Audit Sistem Informasi

Sebagai sebuah *tools*, Sistem informasi ini perlu diaudit. Agar hasil dari sistem informasi ini dapat dijamin mutunya. Adapun tujuan audit sistem informasi menurut Weber (1999: 11-13), dapat disimpulkan secara garis besar terbagi menjadi 5 tahap, yaitu:

1. Meningkatkan keamanan aset-aset perusahaan.

   Aset informasi suatu perusahaan seperti perangkat keras (*hardware*), perangkat lunak (*software*), sumber daya manusia, *file* data harus dijaga oleh suatu sistem pengendalian *intern* yang baik agar tidak terjadi penyalahgunaan aset.

2. Meningkatkan dan menjaga integritas data.

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

3. Meningkatkan efektifitas sistem.

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

4. Meningkatkan efisiensi sistem.

   Efisien sistem menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang memadai.

5. Ekonomis

   Ekonomis mencerminkan kalkulasi untuk rugi ekonomi (*cost/benefit*) yang lebih bersifat kuantifikasi nilai moneter (uang).

Gondodiyoto (2007: 474) menyimpulkan tujuan audit sistem informasi sebagai berikut:

1. Pengamanan Aset,

   Aset informasi suatu perusahaan seperti *hardware, software*, sumber daya manusia (*brainware), file* data harus dijaga oleh suatu sistem pengendalian internal yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset merupakan suatu hal fundamental yang sangat penting yang harus dipenuhi oleh perusahaan.

2. Menjaga Integritas Data,

   Integritas data adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut tertentu seperti: kelengkapan dan keakuratan. Jika tidak terpelihara, maka suatu perusahaan tidak akan lagi memiliki informasi atau laporan yang benar bahkan perusahaan dapat menderita kerugian dari kesalahaan dalam membuat atau mengambil keputusan.

3. Efektifitas Sistem,

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

4. Efisiensi Sistem,

   Efisiensi menjadi hal yang sangat penting suatu komputer tidak lagi memiliki kapasitas yang memadai. 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 dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan *user* dengan sumber daya informasi yang minimal.

5. Ekonomis,

   Ekonomis mencerminkan kalkulasi untuk rugi ekonomi (*cost/benefit*) yang lebih bersifat kuantifikasi nilai moneter (uang).

Dari berbagai definisi di atas penulis menyimpulkan bahwa tujuan audit sistem informasi dapat dikelompokkan ke dalam dua aspek utama dalam pengelolaan teknologi informasi, yaitu:

(1) *Conformance* (kesesuaian)

Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kesesuaian, yaitu: *confidentiality* (kerahasiaan), *integrity* (integritas), *availability* (ketersediaan), dan *compliance* (kepatuhan).

(2) *Performance* (kinerja)

Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kinerja, yaitu: *effectiveness* (efektifitas), *efficiency* (efisiensi), *reliability* (kehandalan).

2.1.8 Pendekatan Audit Sistem Informasi

Menurut Watne (1990), metode pendekatan audit sistem informasi antara lain adalah:

1. *Auditing Around the Computer* (audit sekitar komputer).

   Yaitu dimana penggunaan komputer pada tahap proses diabaikan. 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, auditor melakukan pemeriksaan di sekitar komputer saja. Pendekatan ini juga memiliki beberapa kelemahan, antara lain:

   a. Umumnya *database* mencakup jumlah data yang banyak dan sukar untuk ditelusuri secara manual.
   b. Tidak menciptakan sarana bagi auditor untuk menghayati dan mendalami lebih mantap liku-liku komputer.

c. Pendekatan ini mengabaikan pengendalian sistem dalam pengolahan komputer itu sendiri, sehingga rawan terhadap adanya kelemahan dan kesalahan yang potensial didalamnya.
d. Kemampuan komputer sebagai fasilitas penunjang pelaksanaan audit menjadi kurang dioptimalkan.
e. Tidak dapat mendalami keseluruhan proses audit untuk dapat memaksimalkan hasil audit.

2. *Auditing Through the Computer* (*auditing* melalui komputer).

Yaitu dimana pada tahap proses penggunaan komputer telah aktif. Pendekatan ini lebih menekankan pada langkah pemrosesan serta pengendalian program yang dilakukan oleh sistem komputer. Pendekatan ini mengasumsikan bahwa aspek pengendalian yang memadai, maka kesalahan dan penyimpangan kemungkinan besar tidak terjadi. Pendekatan ini biasanya diterapkan pada sistem pengolahan data *on-line* yang tidak memberikan jejak audit yang memadai.

Pendekatan ini memiliki keuntungan utama yaitu dapat meningkatkan kekuatan terhadap pengujian sistem aplikasi secara efektif, dimana ruang lingkup dan kemampuan dari pengujian yang dilakukan dapat diperluas sehingga tingkat kepercayaan terhadap keandalan dari pengumpulan dan pengevaluasian bukti dapat ditingkatkan.

Pendekatan ini memiliki beberapa kelemahan antara lain:

a. Biaya yang dibutuhkan relatif tinggi yang disebabkan jumlah jam kerja yang banyak untuk dapat lebih memahami struktur kontrol internal dari pelaksanaan sistem aplikasi.
b. Butuh banyak keahlian teknis yang lebih mendalam untuk memahami cara kerja.

3. *Auditing with the Computer* (*auditing* dengan komputer)

Yaitu dimana *input*, proses, dan *ouput* telah menggunakan komputer. Pendekatan ini digunakan untuk mengotomatisasi banyak kegiatan audit. Auditor memanfaatkan komputer sebagai alat bantu dalam melakukan penulisan, perhitungan, pembandingan dan sebagainya. Pendekatan ini menggunakan perangkat lunak *Generalized Audit Software*, yaitu program audit yang berlaku umum untuk berbagai klien.

Keunggulan dari pendekatan ini antara lain:

a. Menggunakan program komputer yang diproses untuk membantu pengujian pengendalian sistem komputer klien itu sendiri secara lebih cepat dan akurat.

b. Dapat melaksanakan tugas audit yang terpisah dari catatan klien, yaitu dengan mengambil *copy data* atau *file* untuk diuji dengan komputer lain.

Pendekatan ini memiliki kelemahan adalah dibutuhkan upaya dan biaya yang *relative* besar untuk pengembangannya.

2.1.9 Sistem Pengendalian Internal

Menurut Weber (1999: 35) "*A control is a sistem that prevents, detects, or corrects unlawful events.*"

Arti dari pernyataan Weber diatas yaitu pengendalian merupakan suatu sistem untuk mencegah, mendeteksi, dan mengoreksi kejadian yang timbul saat transaksi dari serangkaian pemrosesan yang tidak terotorisasi secara sah, tidak akurat, tidak lengkap, mengandung redudansi, tidak efektif, dan tidak efisien.

Menurut *The Information System Control and Audit Association* (ISACA) (2007:65).

> *"Internal control system is the policies, procedures, practices, and organizational structures, designed to provide reasonable assurance that business objectives will be achieved and that undersired events will be prevented, or detected and corrected."*

Maksud dari pernyataan di atas adalah bahwa sistem pengendalian internal merupakan kebijakan, prosedur, praktik-praktik, dan struktur organisasi yang didesain untuk memberikan jaminan yang layak pada upaya pencapaian tujuan bisnis yang akan dicapai dan memastikan kejadian-kejadian yang tidak diinginkan akan dicegah, atau dideteksi dan dikoreksi.

Berdasarkan definisi-definisi yang sudah dijelaskan di atas, maka pengendalian dapat dikelompokkan menjadi tiga bagian, antara lain:

a. *Preventive Controls*

   Instruksi yang ditempatkan pada dokumen sumber untuk mencegah atau menjaga terjadinya kesalahan dalam pengisiannya.

b. *Detective Controls*

   Pengendalian ini digunakan untuk menemukan atau mengetahui bila terjadi kesalahan data yang diinput di dalam sistem.

c. *Corrective Controls*

   Pengendalian yang digunakan untuk memperbaiki masalah yang ditemukan pada *detective control*. *Corrective control* merupakan pengendalian yang terdiri dari program yang menggunakan kode khusus yang dapat memperbaiki data yang rusak atau *error* karena kesalahan pada komunikasi *online*.

Dari definisi-definisi di atas penulis dapat menyimpulkan bahwa sistem pengendalian *internal* merupakan suatu sistem yang dipengaruhi oleh entitas organisasi yang dirancang untuk mencegah, mengendalikan, serta melindungi seluruh aktivitas organisasi dari penyimpangan-penyimpangan atau *undersirable event* lainnya yang dapat merugikan perusahaan dan bertujuan untuk memastikan kepatuhan entitas terhadap peraturan dan kebijakan perusahaan yang akhirnya dapat menciptakan keandalan laporan, keuangan, meningkatkan efektifitas, serta efisiensi operasi perusahaan, dan menjaga aset organisasi.

2.1.10 Tujuan dan Manfaat Sistem Pengendalian Internal

Gondodiyoto (2007: 260) berpendapat bahwa tujuan utama dari sistem pengendalian internal adalah :

1) Mengamankan aset organisasi.
2) Memperoleh informasi yang akurat dan dapat dipercaya.
3) Meningkatkan efektifitas dan efisiensi kegiatan.
4) Mendorong kepatuhan pelaksanaan terhadap kebijaksanaan organisasi.

Berdasarkan pendapat-pendapat di atas, penulis menyimpulkan bahwa tujuan utama dari sistem pengendalian internal adalah untuk menjaga aset perusahaan, meningkatkan efektifitas dan efisiensi operasi perusahaan, mendorong dipatuhinya kebijakan manajemen, mencegah tindakan penyimpangan, dan memperkecil kesalahan.

2.1.11 Tahapan Audit

Dalam melakukan kegiatan audit, tahapan audit menurut Hunton (2004) sebagai berikut:

1. *Planning*, mendapatkan pemahaman yang lengkap mengenai bisnis perusahaan yang sedang dilakukan audit. Pada tahapan ini auditor menentukan ruang lingkup dan tujuan pengendalian, tingkat materialitas, dan *outsourcing*. Pada tahapan ini juga auditor dapat menetapkan mengapa, bagaimana, kapan dan oleh siapa audit akan dilaksanakan. Sebuah program audit awal sudah dipersiapkan dalam mematangkan tahap perencanaan untuk menunjukkan sifat, keluasan, dan waktu prosedur-prosedur yang

dibutuhkan untuk mencapai tujuan audit dan untuk meminimalkan resiko dari audit yang dijalankan.

2. *Risk Assessment*, menganalisis resiko audit dengan menggunakan *risk-based audit approach* agar pengauditan lebih efisien dan masalah *tercover*. Auditor harus memiliki pemahaman mendalam mengenai perushaan, industri, dan lingkungan tempat perusahaan beroperasi, serta hakikat dari proses bisnis perusahaan.
3. *Prepare Audit Program*, audit program disesuaikan dengan *hardware* dan *software* yang dimiliki perusahaan, topologi dan arsitektur jaringan, dan lingkungan serta pertimbangan khusus mengenai industri tersebut. Komponen-komponen dari audit program tersebut adalah ruang lingkup audit, sasaran audit, prosedut audit, serta rincian perencanaan dan pelaporan.
4. *Gather Evidence*, memiliki tujuan untuk mendapatkan bukti-bukti memadai, handal, relevan, dan berguna untuk mencapai sasaran audit secara efektif. Bukti-bukti yang sering ditemukan auditor pada saat kerja lapangan yaitu: observasi proses-proses dan keberadaan dari item fisik seperti pengoperasian komputer ataupun prosedut backup data, bukti-bukti dalam bentuk dokumen (seperti *program change logs, sistem access logs*, dan table otorit*as*), gambaran dari perusahaan (seperti *flowcharts, narretives*, dan kebijakan serta prosedur yang tertulis), analisa (seperti prosedur CAAT(*computer aided auditing technique*) yang dijalankan pada data perusahaan.

5. *Form Conclusion*, digunakan untuk mengevaluasi bukti-bukti dan membuat suatu kesimpulan tentang hasil pemeriksaan yang pada akhirnya akan mengarah pada opini audit. Selain itu, auditor juga akan melaporkan kelemahan maupun kelebihan dari sistem.
6. *Deliver Audit Opinion*, adalah informasi umum yang harus ada dalam sebuah laporan audit seperti:
    a) Nama dari organisasi atau perusahaan yang diaudit.
    b) Judul, tanda tangan dan tanggal.
    c) Pernyataan sasaran audit dan apakah audit tersebut telah memenuhi sasaran.
    d) Ruang lingkup audit, termasuk didalamnya area audit fungsional, periode audit yang tercakup, dan sistem informasi, aplikasi atau lingkungan proses yang diaudit.
    e) Pernyataan bahwa telah terjadi pembatasan ruang lingkup dimana auditor tidak dapat melaksanakan pekerjaan audit dengan memadai untuk mencapai sasaran-sasaran audit tertentu.
    f) Pengguna laporan audit yang dikehendaki termasuk beberapa pembatasan dalam pendistibusian laporan audit.
    g) Standar-standar yang menjadi dasar auditor untuk melaksanakan pekerjaan audit tersebut.
    h) Penjelasan yang terperinci tentang temuan audit yang penting.
    i) Kesimpulan dari area audit yang dievaluasi termasuk syarat dan kualifikasi penting.

j) Saran-saran yang tepat untuk tindakan perbaikan dan peningkatan.

k) Peristiwa-peristiwa penting yang terjadi setelah masa *fieldwork* audit yang bersangkutan berakhir.

7. *Follow Up,* merupakan tindak lanjut dengan ketentuan untuk melakukan tindak lanjut bersama dengan perusahaan pada kondisi-kondisi yang dilaporkan. Tindakan lanjut ini dapat dilakukan dengan menelepon pihak manajemen.

2.1.12 *Control Objectives for Information and Related Technology* (COBIT)

COBIT (*Control Objectives for Information and Related Technology*) dapat definisikan sebagai alat pengendalian untuk informasi dan teknologi terkait dan merupakan standar terbuka untuk pengendalian terhadap teknologi informasi yang dikembangkan oleh *Information System Audit and Control Association* (ISACA) melalui lembaga yang dibentuknya yaitu *Information and Technology Governance Institute* (ITGI) pada tahun 1992. (Sutabri, 2012).

COBIT pertama kali diluncurkan pada tahun 1996, mengalami perubahan berupa perhatian lebih kepada dokumen sumber, revisi pada tingkat lebih lanjut serta tujuan pengendalian rinci dan tambahan seperangkat alat implementasi (*implementation tool set*) pada edisi keduanya yang dipublikasikan pada tahun 1998. COBIT pada edisi ketiga ditandai dengan masuknya penerbit utama baru COBIT yaitu ITGI. COBIT edisi keempat merupakan versi terakhir dari tujuan pengendalian untuk informasi dan teknologi terkait.

Tujuan diluncurkan COBIT adalah untuk mengembangkan, melakukan riset dan mempublikasikan suatu standar teknologi informasi yang diterima umum dan selalu *up to date* untuk digunakan dalam kegiatan bisnis sehari-hari. Dengan bahasa lain, COBIT dapat pula dikatakan sebagai sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu auditor, manajemen dan pengguna (*user*) untuk menjembatani *gap* antara risiko bisnis, kebutuhan kontrol dan permasalahan-permasalahan teknis melalui pengendalian terhadap masing-masing dari 34 proses TI, meningkatkan tingkatan kemapanan proses dalam TI dan memenuhi ekspektasi bisnis dari TI. (Sutabri, 2012).

COBIT mampu menyediakan bahasa yang umum sehingga dapat dipahami oleh semua pihak. Adopsi yang cepat dari COBIT di seluruh dunia dapat dikaitkan dengan semakin besarnya perhatian yang diberikan terhadap *corporate governance* dan kebutuhan perusahaan agar mampu berbuat lebih dengan sumber daya yang sedikit meskipun ketika terjadi kondisi ekonomi yang sulit.

Fokus utama COBIT adalah harapan bahwa melalui adopsi COBIT ini perusahaan akan mampu meningkatkan nilai tambah melalui penggunaan TI dan mengurangi risiko-risiko inheren yang teridentifikasi di dalamnya.

COBIT memiliki beberapa kriteria-kriteria informasi yang menjadi perhatian dari COBIT itu sendiri diantaranya adalah:

a. *Effectiveness* (efektifitas): Informasi yang diperoleh harus relevan dan berkaitan dengan proses bisnis, konsisten, dapat dipercaya, dan tepat waktu.

b. *Efficiency* (efisiensi): Penyediaan informasi melalui penggunaan sumber daya (yang paling produktif dan ekonomis) yang optimal.
c. *Confidentiality* (kerahasiaan): Berkaitan dengan proteksi pada informasi penting dari pihak-pihak yang tidak memiliki hak otorisasi atau tidak berwenang.
d. *Integrity* (integritas): Berkaitan dengan keakuratan dan kelengkapan data atau informasi dan tingkat validitas yang sesuai dengan ekspektasi dan nilai bisnis.
e. *Availability* (ketersediaan): Fokus terhadap ketersediaan data atau informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun di masa yang akan datang. Ini juga terkait dengan pengamanan atas sumber daya yang diperlukan dan terkait.
f. *Compliance* (kepatuhan): Pemenuhan data atau informasi yang sesuai dengan ketentuan hokum, peraturan, dan rencana perjanjian atau kontrak untuk proses bisnis.
g. *Reliability* (handal): Fokus pada pemberian informasi yang tepat bagi manajemen untuk mengoperasikan perusahaa dan pemenuhan kewajiban mereka untuk membuat laporan keuangan.

2.1.13 Pengertian *Responsible Accountable Consulted Informed* (RACI)

Responsible Accountable Consulted Informed (RACI) merupakan sebagai alat pemetaan yang dilakukan oleh auditor dalam metode COBIT. RACI merupakan singkatan dari *Responsible Accountable Consulted Informed*. RACI chart yaitu matriks untuk seluruh aktivitas serta otorisasi keputusan yang harus diambil dalam suatu organisasi yang dikaitkan dengan seluruh pihak yang terlibat. Pengertian RACI menurut ISACA (2007:14) adalah:

- *Responsible* merupakan orang yang melakukan suatu kegiatan atau melakukan pekerjaan.
- *Accountable* merupakan orang yang akhirnya bertanggung jawab dan memiliki otoritas untuk memutuskan suatu perkara.
- *Consulted* merupakan orang yang diperlukan umpan balik atau sarannya dan berkontribusi akan kegiatan tersebut.
- *Informed* merupakan orang yang perlu tahu hasil dari suatu keputusan ataupun tindakan.

Kegunaan dari RACI untuk organisasi atau perusahan yang kita kelola yaitu:

- Mengidentifikasi beban kerja yang telah ditugaskan kepada karyawan tertentu atau departemen.
- Memastikan proses tertentu tidak terlalu dominan serta memastikan bahwa anggota baru dijelaskan tentang peran dan tanggung jawab.

- Menemukan keseimbangan yang tepat antara garis dan tanggung jawab proyek.
- Mendistribusikan kerja antar kelompok untuk mendapatkan efisiensi kerja yang lebih baik.
- Terbuka untuk menyelesaikan konflik dan diskusi.
- Mendokumentasikan peran dan tanggung jawab orang-orang dalam organisasi.

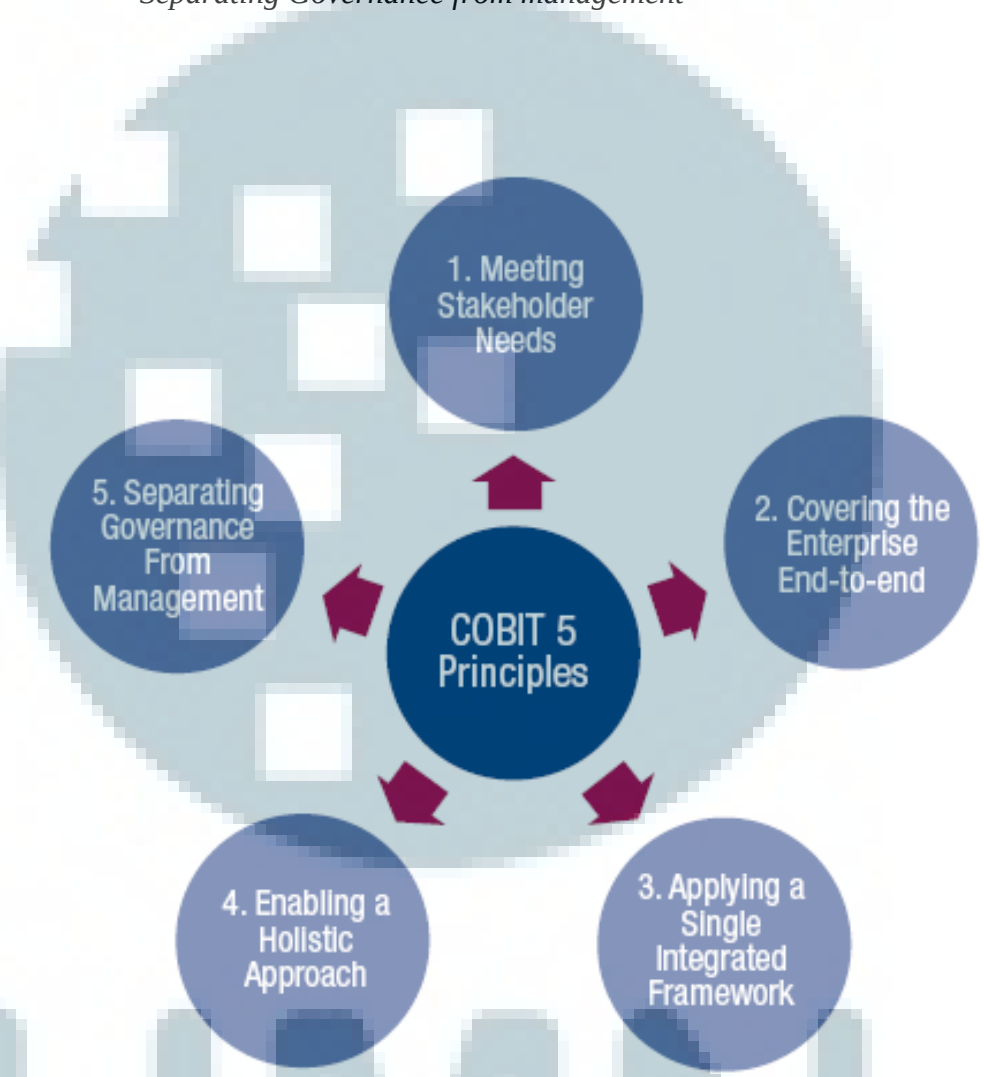
2.1.14 COBIT 5.0

COBIT 5.0 menyediakan kerangka kerja yang komprehensif yang membantu perusahaan untuk mencapai tujuan dan memberikan nilai melalui *governance* yang efektif dan manajemen perusahaan TI. Pada COBIT 5.0 dapat membantu perusahaan menciptakan nilai optimal dari TI dengan menjaga keseimbangan manfaat dan mengoptimalkan tingkat risiko dan penggunaan sumber daya, sehingga memungkinkan informasi dan teknologi yang terkait diatur dan dikelola secara holistik untuk seluruh perusahaan dalam bisnis *end-to-end* dan area fungsional tanggung jawab yang berkaitan dengan kepentingan *TI stakeholder* internal dan eksternal. (COBIT 5, 2010).

Di dalam COBIT 5.0 terdapat prinsip yang berguna untuk perusahaan dari semua ukuran komersial, dan tidak untuk sektor publik. Prinsip-prinsip COBIT 5.0 untuk tata kelola dan manajemen dari *enterprise IT* diantaranya:

- *Meeting stakeholder needs*
- *Covering the enterprise end to end*

- *Applying a single, integrated framework*
- *Enabling a holistic approach*
- *Separating Governance from management*



Gambar 2.1 Principle COBIT 5.0

Sumber: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved

Prinsip 1: *Meeting Stakeholder Needs.* Prinsip ini digunakan untuk menciptakan nilai tertentu untuk perusahaan dengan cara mempertahankan serta menyeimbangkan keuntungan dan juga melakukan pengoptimalan resiko dan

penggunaan sumber daya. Pada COBIT 5.0, telah disediakan proses-proses dan juga *Enable* yang diperlukan untuk menciptakan bisnis yang baik melalui penggunaan TI, karena setiap perusahaan memiliki tujuan yang berbeda-beda maka masing-masing perusahaan tersebut dapat menyesuaikan sendiri dengan COBIT 5.0.

Prinsip 2: *Covering the Enterprise End-to-End*. Mencakup seluruh fungsi dan proses yang digunakan dalam perusahaan. COBIT 5.0 tidak berfokus hanya di fungsi TI saja, melainkan memperlakukan informasi dan teknologi yang terkait menjadi salah satu aset yang harus ditangani seperti layaknya aset lainnya.

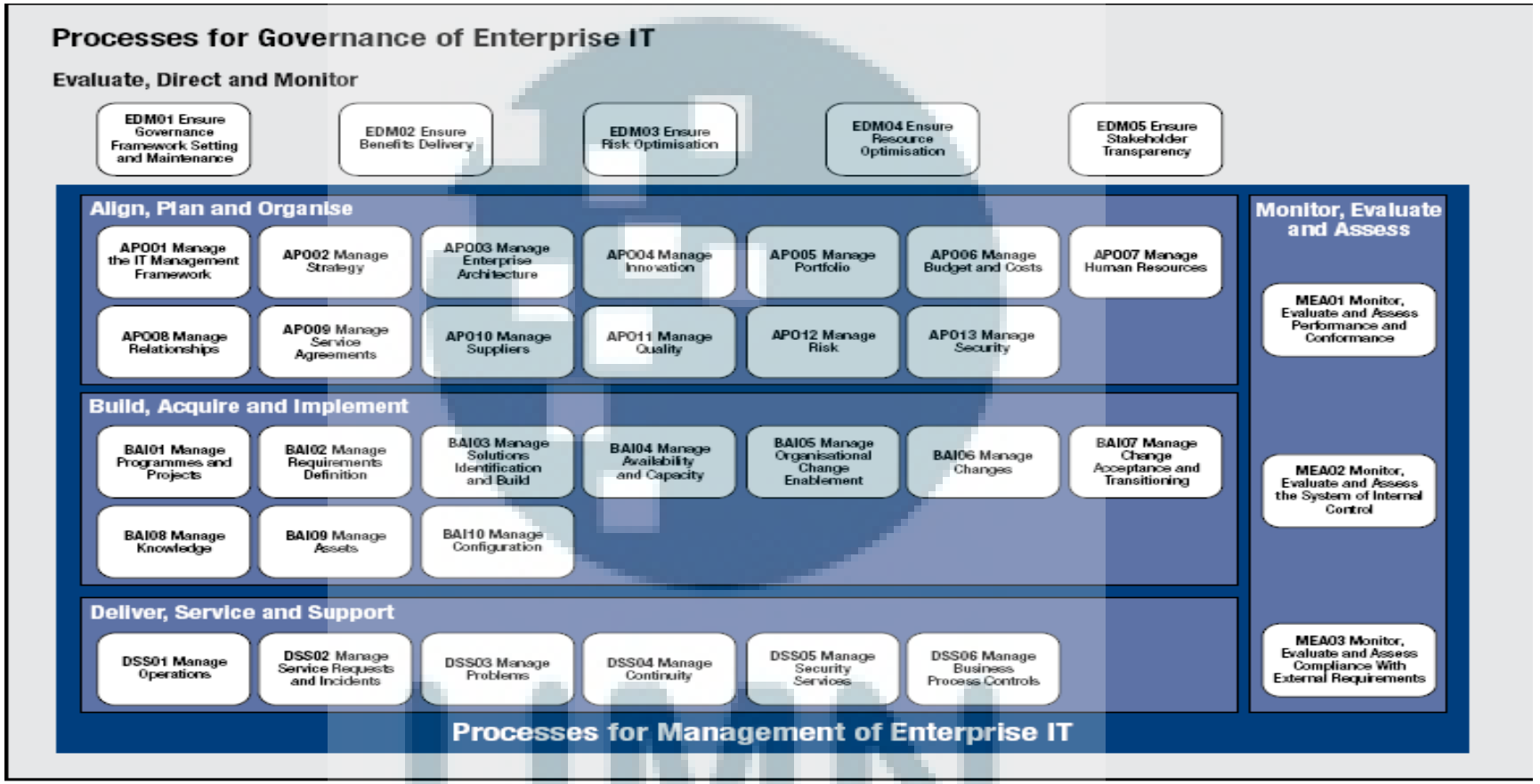
Prinsip 3: *Applying a Single, Integrated Framework.* Ada banyak standar yang berkaitan dengan TI dan *best practices,* dimana masing-masing memberikan arahan dari kegiatan TI. COBIT 5.0 menjadi standar yang relevan dan *framework* tingkat tinggi, dan oleh sebab itu COBIT 5.0 dapat menjadi *framework* yang menyeluruh untuk tata kelola manajemen TI.

Prinsip 4: *Enabling a Holistic Approach.* COBIT 5.0 mendifinisikan satu set *Enabler* untuk mendukung pelakasanaan tata kelola manajemen TI yang komprehensif, dalam hal ini *Enabler* didefinisikan sebagai sesuatu yang dapat membantu perusahaan dalam mencapai tujuannya. Berikut ini merupakan tujuh macam *Enabler,* yaitu:

- Prinsip, kebijakan dan *framework.*
- Proses.
- Struktur Organisasi.
- Etika, Budaya, dan Perilaku.

- Informasi.
- Jasa, Infrastruktur dan Aplikasi.
- Manusia, Kemampuan dan Kompetensi.

Prinsip 5: *Separating Governance From Management.* Pada *framework* dari cobit 5.0, dibuat perbedaan yang sangat jelas antara *Governance* dan juga manajemen. Kedua hal tersebut mencakup kegiatan aktivitas yang berbeda, membutuhkan struktur organisasi yang berbeda juga, dan digunakan untuk memenuhi tujuan yang berbeda.



Gambar 2.2 Enabling Processes

Sumber: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved

Gambar 2.2 adalah gambar *enabling* proses yang dimiliki cobit 5.0, terdiri dari lima *Enabler* dan juga tiga puluh tujuh proses yang merupakan keseluruhan proses dari kelima *Enabler* tersebut. Berikut ini merupakan lima *Enabler* yang digunakan pada COBIT 5.0, yaitu:

- ***Evaluate, Direct, and Monitor***

  Governance memastikan bahwa tujuan perusahaan dapat tercapai dengan melakukan evaluasi kebutuhan dan kondisi dari kebutuhan *stakeholder*, melakukan pengarahan terhadap tujuan perusahaan yang menjadi prioritas dan sebagai penetapan atau pengambilan keputusan. *Monitoring* dilakukan terhadap performa, pemenuhan kebutuhan, dan terhadap progress yang sudah disetujui.

Tabel 2.1 Domain Evaluate, Direct, and Monitoring

EDM01	Pastikan Tata Pengaturan Kerangka dan Pemeliharaan.
EDM02	Pastikan Pengiriman Manfaat.
EDM03	Pastikan Optimisasi Resiko.
EDM04	Pastikan Pengoptimalan Sumber Daya.
EDM05	Pastikan Transparansi *Stakeholder*.

- **EDM01 Pastikan Tata Pengaturan Kerangka dan Pemeliharaan**

  Proses ini memastikan bagian TI diawasi secara efektif dan transparan, juga memastikan keputusan dibuat sejalan dengan strategi dan tujuan perusahaan. Pada proses ini juga disediakan pendekatan yang konsisten dan teritegrasi dengan pendekatan tata kelola perusahaan, sehingga keputusan perusahaan dan

bagian TI dapat diawasi sesuai dengan hukum dan persyaratan peraturan yang telah dikonfirmasi serta persyaratan yang telah dipenuhi dewan anggota tata kelola.

- **EDM02 Pastikan Pengiriman Manfaat**

  Pengoptimalan kontribusi dari nilai bisnis, layanan TI, dan aset TI dari investasi dengan biaya yang dapat diterima dengan tujuan dari adanya proses ini dapat mengamankan nilai yang optimal dari TI-*enabled*, menghemat biaya pengiriman solusi, memberikan hasil yang akurat, serta biaya yang dikeluarkan dapat dimanfaatkan agar kebutuhan bisnis dapat berjalan secara efektif dan efisien.

- **EDM03 Pastikan Optimisasi Resiko**

  Proses yang bertujuan untuk memastikan bahwa resiko perusahaan tidak melebihi toleransi dari resiko *appetite* dan dampak dari resiko TI dapat diidentifikasi dan dikelola dengan cara meminimalisasikan potensi kegagalan yang mungkin terjadi.

- **EDM04 Pastikan Pengoptimalan Sumber Daya**

  Memastikan kemampuan TI yang tersedia dapat memadai untuk mendukung tujuan perusahaan akan sumber yang dibutuhkan

dapat dipenuhi secara optimal dan untuk kesiapan perubahan masa depan.

- **EDM05 Pastikan Transparansi *Stakeholder***

  Tujuan proses ini yaitu untuk membuat dasar pelaporan dengan tujuan untuk meningkatkan kinerja perusahaan dengan cara memastikan bahwa komunikasi kepada *stakeholder* efektif dan tepat waktu, serta proses ini digunakan untuk mengkonfirmasi bahwa tujuan dan strategi TI sejalan dengan tujuan dan strategi perusahaan.

- ***Align, Plan, And Organize***

  Merupakan domain yang mengarahkan suatu perusahaan untuk dapat menggunakan informasi dan teknologi dengan cara paling baik yang dapat digunakan perusahaan tersebut. Pada domain ini juga dibuat perencanaan demi tercapainya tujuan yang telah diarahkan tersebut. Kemudian melakukan *organizing* terhadap perencanaan tersebut sesuai dengan arahan yang telah ada agar mencapai hasil yang optimal.

Tabel 2.2 Domain Align, Plan and Organize

APO01	Mengelola Kerangka Manajemen TI
APO02	Kelola Strategi
APO03	Kelola Enterprise Arsitektur
APO04	Kelola Inovasi
APO05	Kelola Portofolio
APO06	Kelola Anggaran dan Biaya
APO07	Kelola Hubungan Manusia
APO08	Kelola Hubungan
APO09	Kelola Perjanjian Layanan
APO10	Kelola Pemasok
APO11	Kelola Kualitas
APO12	Kelola Risiko
APO13	Kelola Keamanan

- **APO01 Mengelola Kerangka Manajemen TI**

  Proses ini digunakan untuk memperjelas dan juga menjaga tata kelola TI melalui visi dan misi perusahaan dengan cara menyediakan pendekatan manajemen yang konsisten untuk mengaktifkan persyaratan dari tata kelola perusahaan yang harus dipenuhi, seperti proses manajemen struktur organisasi, keterampilan, kompetensi, peran dan tanggung jawab.

- **APO02 Kelola Strategi**

  Melakukan analisis terhadap bisnis dan TI dengan memanfaatkan arsitektur perusahaan dan pihak eksternal sebagai bantuan untuk mengetahui strategi dimasa depan.

- **APO03 Kelola Enterprise Arsitektur**

  Membuat arsitektur umum yang terdiri dari proses bisnis, informasi, data, aplikasi dan lapisan arsitektur teknologi yang efektif dan efisien untuk mewujudkan strategi TI yang bertujuan untuk membentuk hubungan antar prinsip dari desain dan juga evaluasi dari waktu ke waktu.

- **APO04 Kelola Inovasi**

  Menjaga kesadaran akan teknologi informasi dengan melakukan identifikasi terhadap peluang inovasi dan perencanaan untuk mendapatkan keuntungan dari inovasi tersebut yang digunakan untuk kebutuhan bisnis. Proses ini memiliki tujuan untuk dapat memiliki keunggulan kompetitif dengan cara melakukan inovasi dan juga memanfaatkan perkembangan teknologi informasi secara efektif dan efisien.

- **APO05 Kelola Portofolio**

  Proses yang memiliki tujuan untuk mengoptimalkan kinerja program dalam menanggapi kinerja pelayanan dan mengubah prioritas perusahaan dengan cara membuat strategi untuk investasi serta melakukan pertimbangan terhadap kategori yang akan diinvestasikan sumber dayanya.

- **APO08 Kelola Hubungan**

  Melakukan kelola hubungan antara bisnis dan TI untuk memastikan pencapaian tujuan secara bersama-sama dan memberikan hasil yang terbaik dalam mencapai strategi perusahaan. Tujuan proses ini yaitu meningkatkan kepercayaan TI, kepercayaan diri dan penggunaan sumber daya secara efektif.

- **APO09 Kelola Perjanjian Layanan**

  Proses ini digunakan untuk memastikan bahwa tingkat layanan TI memenuhi kebutuhan perusahaan pada saat ini dan masa mendatang. Dalam melakukan pemastian terhadap tingkat layanan TI maka dilakukan dengan cara mengidentifikasi secara spesifik desain layanan, perjanjian, melakukan pengawasan terhadap tingkat layanan TI dan indikator Kinerja.

- **APO10 Kelola Pemasok**

  Pengelolaan TI yang terkait dengan layanan pemasok yang digunakan untuk memenuhi kebutuhan perusahaan dan pengelolaan tersebut antara lain dengan cara memilih pemasok serta menjaga hubungan kontrak manajemen, dan meninjau kinerja pemasok terkait dengan efektifitas dan kepatuhan.

- **APO11 Kelola Kualitas**

  Melakukan pendefinisian terhadap syarat mutu dari proses, prosedur pemantauan, dan standar efisiensi. Proses ini bertujuan memastikan pengiriman agar tetap konsisten dan berada pada mutu yang baik, serta sebagai pemenuhan persyaratan suatu perusahaan untuk memenuhi kebutuhan *stakeholder*.

- **APO12 Kelola Resiko**

  Melakukan pengelolaan terhadap resiko TI agar tetap berada pada batas toleransi manajemen. Tujuan dari proses ini adalah untuk menyeimbangkan biaya dan manfaat pengelolaan TI yang terkait dengan resiko perusahaan.

- **APO13 Kelola Keamanan**

  Mengawasi sistem sebagai bentuk manajemen terhadap keamanan informasi perusahaan. Proses ini bertujuan untuk mengurangi resiko yang dapat terjadi kepada keamanan informas perusahaan.

- ***Build, Acquire, and Implement***

  Mengidentifikasi kebutuhan TI melalui proses bisnisnya yang sedang berjalan pada perusahaan. Proses ini juga melakukan

pemeliharaan sistem untuk dapa memastikan bahwa proses bisnis yang ada sudah efisien dan efektif.

Tabel 2.3 Domain Build, Acquire, dan Implement

BAI01	Kelola Pogram dan Proyek
BAI02	Kelola Definisi Persyaratan
BAI03	Kelola Identifikasi Solusi dan Membangun
BAI04	Kelola Ketersediaan dan Kapasitas
BAI05	Kelola Pemberdayaan Perubahan Organisasi
BAI06	Kelola Perubahan
BAI07	Kelola Penerimaan Perubahaan dan Transisi
BAI08	Kelola Pengetahuan
BAI09	Kelola Aset
BAI10	Kelola Konfigurasi

- **BAI01 Kelola Program dan Proyek**

  Melakukan pengelolaan terhadap program dan proyek yang merupakan strategi perusahaan. Pengelolaan tersebut dapat berupa melakukan control program, menjalankan program dari suatu proyek dan melakukan analisis setelah diimplementasi. Tujuan dari proses ini adalah untuk memastikan nilai dan kualitas dari proyek agar dapat memaksimalkan investasi perusahaan.

- **BAI02 Kelola Definisi Persyaratan**

  Melakukan identifikasi untuk memastikan kesesuaian syarat sebelum akuisisi. Identidikasi tersebut meliputi analisis terhadap proses bisnis, aplikasi, informasi, infrastruktur, dan jasa. Tujuan dari proses ini adalah agar dapat menciptakan solusi yang

digunakan untuk memenuhi kebutuhan perusahaan dan untuk meminimalkan resiko.

- **BAI03 Kelola Identifikasi Solusi dan Membangun**

  Mengelola solusi sesuai dengan persyaratan yang diberikan perusahaan yang meliputi desain, pengembangan, pengadaan, dan bekerja sama dengan pemasok dengan cara melakukan konfigurasi manajemen dan pemeliharan perusahaan.

- **BAI04 Kelola Ketersedian dan Kapasitas**

  Melakukan pengelolaan terhadap kebutuhan saat ini dan kebutuhan untuk masa mendatang, melakukan peramalan atau *forecast* terhadap kebutuhan dimasa mendatang melalui analisis kebutuhan bisnis serta analisis untuk dapat merencanakan tindakan yang dapat digunakan untuk mencegah resiko tersebut. Proses ini bertujuan untuk menjaga ketersediaan dan menyeimbangkan sumber daya agar dapat dioptimalisasikan untuk masa mendatang secara efisien.

- **BAI05 Kelola Pemberdayaan Perubahaan Organisasi**

  Memaksimalkan implementasi pengurangan resiko untuk melakukan perubahaan organisasi perusahaan dan juga

melakukan perubahaan bisnis dengan mengurangi resiko kegagalan.

- **BAI06 Kelola Perubahan**

  Mengelola perubahan standar dengan cara melakukan penilaian terhadap dampak dilakukannya suatu ketetapan, perubahaan darurat, pelacakan pelaporan, dan dokumentasi. Proses ini bertujuan untuk dapat melakukan respon dengan cepat untuk melakukan perubahan bisnis dan juga pengurangan resiko yang berdampak negate.

- **BAI07 Kelola Penerimaan Perubahaan dan Transisi**

  Membuat solusi untuk operasional perencanaan, konversi data, promosi untuk produksi, dan produksi TI dengan melakukan pengamatan setelah dilakukan implementasi. Proses ini memiliki tujuan untuk memberikan solusi yang digunakan untuk dapat mencapai hasil yang diharapkan.

- **BAI08 Kelola Pengetahuan**

  Merupakan proses untuk memberikan pengetahuan yang digunakan untuk mendukung staf dalam pekerjaan dan juga untuk membantu dalam pengambilan keputusan dan meningkatkan produktivitas dengan cara memfasilitasi

pengambilan keputusan serta membuat rencana untuk identifikasi dengan cara memberikan ketersediaan sarana pengetahuan yang relevan, divalidasi dan dapat diandalkan.

- **BAI09 Kelola Aset**

  Memastikan pengguna memberikan biaya optimal sesuai dengan tujuan serta melakukan pencatatan dan melindungi aset penting dalam mendukung TI untuk dapat mengoptimalkan nilai dari aset tersebut.

- **BAI10 Kelola Konfigurasi**

  Memberikan informasi mengenai aset agar dapat dikelola secara efektif dan memelihara hubungan antara sumber daya yang diperlukan untuk memberikan layanan TI-*enabled*, dengan melakukan pengumpulan informasi konfigurasi, verifikasi audit, dan pembaharuan konfigurasi.

- ***Deliver, Service, and Support***

  Merupakan pengiriman eksekusi terhadap aplikasi didalam teknologi informasi yang berada di dalam sistem TI yang digunakan untuk membuat pelaksanaan sistem TI tersebut menjadi efektif dan efisien.

Tabel 2.4 Domain Deliver, Service, and Support

DSS01	Kelola Operasi
DSS02	Kelola Permintaan Layanan dan Insiden
DSS03	Kelola Masalah
DSS04	Kelola Continuity
DSS05	Kelola Jasa Keamanan
DSS06	Kelola Kontrol Proses Bisnis

- **DSS01 Kelola Operasi**

  Melakukan koordinasi terhadap prosedur operasional yang dibutuhkan layanan internal TI dengan melakukan pelaksanaan prosedur standar yang dilakukan dengan tujuan untuk dapat mencapai hasil yang ditargetkan oleh operasional TI.

- **DSS02 Kelola Permintaan Layanan dan Insiden**

  Merespon permintaan berdasarkan jenis insiden, mengatasi situasi agar kembali normal dengan cara merekam dan memenuhi permintaan pengguna, melakukan penyelidikan untuk mengatasi terjadinya peningkatan insiden. Proses ini bertujuan untuk meningkatkan produktivitas dan meminimalkan gangguan terhadap permintaan pengguna dan insiden yang terjadi.

- **DSS03 Kelola Masalah**

  Melakukan identifikasi dan klasifikasi masalah agar dapat diketahui akar masalah dan memberikan solusi tepat pada waktunya. Proses ini bertujuan untuk mencegah masalah yang

sama kembali terulang dan memberikan rekomendasi terhadap masalah serta mengurangi biaya dan juga meningkatkan kenyamanan maupun kepuasan pelanggan dengan mengurangi jumlah masalah operasional.

- **DSS04 Kelola *Continuity***

  Mempertahankan dan menguatkan rencana untuk bisnis TI dapat menanggapi permasalahan yang terjadi dengan cara menjaga ketersediaan informasi. Proses ini memiliki tujuan untuk mempertahankan ketersediaan informasi ketika terjadi gangguan.

- **DSS05 Kelola Jasa Keamanan**

  Melakukan perlindungan terhadap keamanan informasi perusahaan sesuai dengan kebijakan keamanan. Proses ini memiliki tujuan untuk meminimalkan dampak kerentanan dari keamanan informasi operasional dengan cara membangun dan memelihara keamanan informasi dan hak akses untuk dilakukannya pemantauan keamanan.

- **DSS06 Kelola Kontrol Proses Bisnis**

  Melakukan pemeliharaan agar integitas informasi dan keamanan aset informasi dapat terjaga serta melakukan identifikasi informasi dengan mengelola dan mengoperasikan agar dapat dipastikan bahwa informasi dan pengelohan informasi tersebut memenuhi persyaratan.

- ***Monitor dan Evaluate Assess***

  Digunakan untuk memastikan seluruh proses berjalan diarah yang telah diberikan sehingga hasilnya sesuai dengan apa yang sudah ditargetkan. Pemantauan tersebut mencakup penilaian terhadap efektifitas kemampuan dari sistem sebagai pemenuhan tujuan perusahaan. Proses tersebut dikontrol oleh auditor internal ataupun eksternal.

Tabel 2.5 Domain Monitor, Evaluate, and Assess

MEA01	Memantau dan Mengevaluasi, Menilai Kinerja dan Kesesuaian.
MEA02	Memantau, evaluasi dan Asses Sistem Pengendalian Internal.
MEA03	Mengevaluasi dan Menilai Kepatuhan dengan Persyaratan Eksternal.

- **MEA01 Memantau dan Mengevaluasi, Menilai Kinerja dan Kesesuaian**

  Mengumpulkan, melakukan validasi dan evaluasi dari proses bisnis TI yang digunakan untuk memberikan transparansi kinerja, kesesuaian, dan pencapaian tujuan yang telah disepakati.

- **MEA02 Memantau, Evaluasi, dan *Asses* Sistem Pengendalian Intern**

  Memantau dan melakukan evaluasi terhadap lingkungan yang memungkinkan manajemen untuk mengidentifikasi ketidakefisienan yang terjadi sehingga dapat dilakukan tindakan perbaikan, perencanaan, mengatur kegiatan dan menjaga standar penilaian pengendalian internal. Proses ini memiliki tujuan untuk dapat memberikan kepercayaan operasional terhadap pencapaian tujuan perusahaan dan pemahaman terhadap resiko yang belum teratasi.

- **MEA03 Mengevaluasi dan Menilai Kepatuhan dengan Persyaratan Eksternal**

  Penilaian proses TI dari undang-undang, peraturan, dan persyaratn kontrak yang digunakan untuk dapat meyakinkan bahwa persyaratan telah dipenuhi sesuai dengan kebijakan

perusahaan secara keseluruhan dan memastikan agar perusahaan tersebut kompatibel.

2.1.15 *Capability Level*

COBIT 5.0 meliputi *process capability level* yang berdasarkan pada ISO/IEC 15504 yang telah diakui secara internasional. Model ini akan mencapai tujuan secara keseluruhan penilaian proses dan mendukung proses perbaikan, yaitu akan menyediakan sarana untuk mengukur kinerja dari setiap proses tata kelola atau manajemen proses dan akan memungkinkan area perbaikan dapat teridentifikasi. Skala peringkat dari *process capability level* ini melibatkan enam tingkat kemampuan, antara lain: (COBIT 5, 2010)

1. Level 0, *Incomplete Process*: Proses ini tidak dilaksanakan atau gagal untuk mencapai tujuan prosesnya. Pada tingkat ini, ada sedikit bukti atau bahkan tidak ada bukti setiap pencapaian sistematis dari tujuan proses.
2. Level 1, *Performed Process (one attribute)*: Proses dilaksanakan dan mencapai tujuan prosesnya.
3. Level 2, *Managed Process (two attributes)*: Proses yang dilakukan sekarang diimplementasikan, dikelola (direncanakan, dimonitor, dan disesuaikan) dan produk kerja yang tepat ditetapkan, dikendalikan dan dipelihara.
4. Level 3, *Established Process (two attributes)*: Proses yang dikelola kini diterapkan menggunakan proses yang telah ditetapkan yang mampu mencapai hasil prosesnya.

5. Level 4, *Predictable Process (two attributes)*: Proses yang ditetapkan sekarang beroperasi dalam batas yang telah ditetapkan untuk mencapai hasil prosesnya.
6. Level 5, *Optimizing Process (two attributes)*: Proses diprediksi untuk terus ditingkatkan untuk memenuhi tujuan bisnis yang relevan saat ini dan tujuan bisnis di masa yang akan datang.

Process capability level menggunakan skala peringkat ISO/IEC 15504 untuk menetapkan peringkat masing-masing tujuan hingga tercapai. Peringkat ini seperti dijelaskan pada tabel 2.6 dibawah ini:

Tabel 2.6 Persentase Peringkat

Abbreviation	***Description***	***% Achieved***
N	*Not achieved*	*0 to 15% achievement*
P	*Partially achieved*	*>15% to 50% achievement*
L	*Largely achieved*	*>50% to 85% achievement*
F	*Fully achieved*	*>85% to 100% achievement*

1. ***Not achieved***

   Terdapat sedikit bukti atau bahkan tidak ada bukti dari pencapaian atribut yang ditetapkan pada proses yang dinilai.
2. ***Partially achieved***

   Terdapat beberapa bukti dan beberapa pencapaian dari atribut yang ditetapkan pada proses yang dinilai. Beberapa aspek pencapaian atribut mungkin tidak dapat diprediksi.
3. ***Largely achieved***

Terdapat bukti pendekatan sistematis untuk proses yang dinilai dan terdapat pencapaian yang signifikan. Beberapa kelemahan terkait dengan atribut ini mungkin ada dalam proses yang dinilai.

4. ***Fully achieved***

   Terdapat bukti dari pendekatan yang lengkap dan sistematis dari atribut yang ditetapkan dalam proses yang dinilai. Terdapat bukti dari pendekatan yang lengkap dan sistematis terhadap pencapaian keseluruhan. Tidak ada kelemahan signifikan yang berhubungan dengan atribut ini ada dalam proses dinilai.

Dalam melakukan proses penilaian *capability level* proses COBIT, masing-masing proses dicek secara bertahap apakah proses tersebut telah memenuhi persyaratan-persyaratan yang harus dipenuhi pada masing-masing level, mulai dari level 1 hingga level 5. Selain itu, terdapat ketentuan kategori dari hasil penilaian ditiap levelnya, yaitu suatu proses cukup meraih kategori *largely achieved* (L) dengan range nilai berkisar 50-85% atau *fully achieved* (F) dengan range nilai berkisar 85%-100% untuk dapat dinyatakan bahwa proses tersebut telah meraih suatu level kapabilitas tersebut, namun proses tersebut harus meraih kategori *fully achieved* (F) untuk dapat melanjutkan penilaian ke level kapabilitas berikutnya.

2.1.16 Metode Pengumpulan Data

Menurut Sugiyono (2004: 130), Teknik pengumpulan data ada tiga, yaitu:

1. Wawancara

   Wawancara digunakan apabila peneliti ingin melakukan studi pendahuluan untuk menemukan permasalahan yang harus diteliti, dan juga apabila peneliti ingin mengetahui hal-hal dari responden yang lebih mendalam dan jumlah respondennya sedikit.

2. Kuesioner

   Kuesioner merupakan teknik yang dilakukan dengan cara memberi seperangkat pertanyaan tertulis kepada responden untuk dijawabnya. Kuesioner merupakan teknik pengumpulan data yang efisien bila peneliti tahu dengan pasti variable yang akan diukur dengan tahu apa yang dapat diharapkan dari responden.

3. Observasi

   Observasi mempunyai ciri yang spesifik bila dibandingkan dengan teknik yang lain. Jika wawancara dan kuesioner selalu berkomunikasi dengan orang, maka observasi tidak terbatas pada orang tetapi juga objek-objek alam yang lain. Teknik ini digunakan bila penelitian berkenaan dengan perilaku manusia, proses kerja, gejala-gejala alam, dan bila responden yang diamati tidak terlalu besar.

2.1.17 Penilaian Risiko

Menurut COSO, penilaian risiko melibatkan proses yang dinamis dan interaktif untuk mengidentifikasi dan menilai risiko terhadap pencapaian tujuan. Risiko itu sendiri dipahami sebagai suatu kemungkinan bahwa suatu peristiwa akan terjadi dan mempengaruhi pencapaian tujuan entitas, dan risiko terhadap pencapaian seluruh tujuan dari entitas ini dianggap relatif terhadap toleransi risiko yang ditetapkan. Oleh karena itu, penilaian risiko membentuk dasar untuk menentukan bagaimana risiko harus dikelola oleh organisasi. (Hall, 2013).

Prinsip-prinsip yang mendukung penilaian risiko adalah sebagai berikut:

a. Organisasi menetapkan tujuan dengan kejelasan yang cukup untuk memungkinkan identifikasi dan penilaian risiko yang berkaitan dengan tujuan.
b. Organisasi mengidentifikasi risiko terhadap pencapaian tujuan diseluruh entitas dan analisis risiko sebagai dasar untuk menentukan bagaimana risiko sebagai dasar untuk menentukan bagaimana risiko harus dikelola.
c. Organisasi mempertimbangkan potensi kecurangan dalam menilai risiko terhadap pencapaian tujuan.
d. Organisasi mengidentifikasi dan menilai perubahaan yang signifikan dapat mempengaruhi sistem pengendalian.

Tahap penilaian risiko dalam audit terdiri dari : (Tuanakotta, 2013).

1. Melangsungkan penerimaan klien atau prosedur pelanjutan.
2. Merencanakan peningkatan secara keseluruhan.

3. Menunjukkan prosedur penilaian risiko untuk pemahaman bisnis dan mengidentifikasi risiko pengendalian dan inheren.
4. Mengidentifikasi prosedur pengendalian internal yang relevan dan menilai desain dan implementasi mereka.
5. Mengidentifikasi risiko yang signifikan yang memerlukan pertimbangan khusus audit dan risikonya untuk prosedur itu sendiri yang tidak memenuhi.
6. Komunikasi materi kelemahan dalam desain dan pelaksanaan pengendalian internal untuk manajemen dan orang yang dituntut dengan pemerintahan.
7. Membuat sebuah informasi penilaian terhadap risiko dari salah saji materi pada semua tingkatan laporan keuangan dan tingkatan asersi.