BAB II

TELAAH LITERATUR

2.1 Auditing

2.1.1 Definisi Auditing

Kata audit berasal dari bahasa latin yaitu *audiere* yang berarti dengar (*hear*). Auditing menurut Messier, et al (2006:16) merumuskan definisi umum dari audit "*Auditing* adalah suatu proses sistematis mendapatkan dan mengevaluasi bukti-bukti secara objektif sehubungan dengan asersi atas tindakan dan peristiwa ekonomi untuk memastikan tingkat kesesuaian antara asersi-asersi tersebut dan menetapkan kriteria serta mengkomunikasikan hasilnya kepada pihak-pihak yang berkepentingan."

Menurut Agoes (2004:3), definisi auditing adalah : "Suatu pendekatan yang dilakukan secara kritis dan sistematis, oleh pihak independen, terhadap laporan keuangan yang telah disusun oleh manajemen, beserta catatan-catatan pembukuan dan bukti-bukti pendukungnya, dengan tujuan untuk dapat memberikan pendapat mengenai kewajaran laporan keuangan tersebut."

Menurut Mulyadi (2002:9), definisi auditing secara umum adalah : "Suatu proses sistematis untuk memperoleh dan mengevaluasi bukti

secara objektif mengenai pernyataan-pernyataan tentang kejadian ekonomi dengan tujuan-tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan".

Auditing menurut Arens, et al (2005:11) menyatakan bahwa, "*Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established kriteria. Auditing should be done by a competent, independent person.*"

Dari pengertian diatas dapat disimpulkan bahwa auditing memiliki beberapa komponen penting, diantaranya :

- Proses secara sistematis, dapat diartikan bahwa auditing merupakan suatu kegiatan yang dilakukan dengan tahapan tertentu dan terstruktur dalam sebuah *framework* yang jelas.
- Informasi yang terukur dan kriteria yang telah ditetapkan, maksudnya adalah bahwa dalam pemeriksaan keuangan, auditor memerlukan informasi-informasi yang dapat dibuktikan kebenarannya dan juga membutuhkan kriteria atau standar yang dapat dijadikan pegangan dalam mengevaluasi informasi tersebut.

- Menghimpun dan mengevaluasi bukti-bukti yang ada, bukti (*evidence*) merupakan suatu informasi utama yang digunakan oleh auditor dalam menentukan kesesuaian informasi yang diaudit dengan kriteria atau standar yang telah ditetapkan.

- Kompeten dan independen, kompeten yang dimaksud adalah bahwa seorang auditor harus benar-benar menguasai bidangnya sehingga dapat mengerjakan tugasnya dengan baik. Independen diartikan sebagai sikap mental yang harus dimiliki oleh seorang auditor dimana ia memiliki kebebasan untuk melakukan audit yang handal.

- Pelaporan, merupakan tahap paling akhir dalam melaksanakan proses audit. Di dalam laporan ini berisikan hasil dari audit yang dilakukan yang selanjutnya akan diberikan kepada pihak yang berkepentingan sebagai informasi

2.2 Sistem Informasi

2.2.1 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 (2006:4) , *"A system is a set of two or more interrelated componenets that interact to achieve a goal.*

Dari dua pendapat diatas dapat disimpulkan bahwa sistem adalah elemen atau komponen yang terintegrasi untuk mencapai tujuan tertentu.

2.2.2 Definisi Informasi

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

Menurut Romney dan Steinbart (2006:5), *"Information is data that have been organized and processed to provide meaning to a user."*

Dari dua pengertian diatas dapat diambil kesimpulan bahwa informasi akan lebih bermanfaat bagi penggunannya jika sudah diolah.

2.2.3 Definisi Sistem Informasi

Hall (2001:7) mendefinisikan "Sistem informasi sebagai sebuah rangkaian prosedur formal dimana data dikelompokkan, diproses menjadi informasi, dan didistribusikan kepada pemakai".

O'Brien (2005:5) mendefinisikan "*Information sistem can be any organized combination of people, hardware, software, communication networks, and data resource that collect, transform, disseminates information in an organization"*.

Dapat disimpulkan bahwa "Sistem informasi adalah suatu kesatuan yang terdiri dari manusia (*brainware*), perangkat keras (*hardware*), perangkat lunak (*software*), jaringan komputer (*network*), dan kumpulan data yang bermanfaat untuk mengumpulkan, mentransformasikan dan mendistribusikan informasi didalam suatu organisasi".

2.3 Audit Sistem Information (SI)

2.3.1 Definisi Audit SI

Definisi Information Sistem menurut Weber (1999:10), *"Information sistems auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to beachieved effectively, and uses resources efficiently"*.

Menurut Cangemi (2003:48),"*Information sistems auditing is Defined as any audit that encompass the review and evaluation of all aspects (or any portion) ofautomated information processing sistems, including related non-automated processes, and the interfaces between them"*.

Gondodiyoto (2003:151) berpendapat bahwa,"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, memiliki mekanisme pengamanan asset yang memadai, serta menjamin integritas data yang memadai".

Dari 3 pendapat diatas dapat disimpulkan bahwa audit sistem informasi adalah suatu proses pengumpulan dan pengevaluasian terhaap barang bukti untuk mengetahui tingkat kesesuaian antara berjalannya apliaksi pada perusahaan dengan aturan atau prosedur yang telah dibuat.

2.3.2 Tujuan Audit Sistem Informasi

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 kesalahan 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 ketika 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). Efisien yang berarti sumber daya.

2.3.3 Pendekatan Audit Sistem Informasi

Menurut Weber (1999:55-57), terdapat beberapa metode pendekatan audit sistem informasi, yaitu:

1. *Auditing around the computer*

   Merupakan suatu pendekatan audit dengan memperlakukan komputer sebagai *black box*, maksudnya metode ini tidak menguji langkah-langkah proses secara langsung, tetapi hanya berfokus pada *input* dan *output* dari sistem komputer. Diasumsikan bahwa jika *input* benar akan diwujudkan pada *output*, sehingga pemrosesannya juga benar dan tidak melakukan pengecekan terhadap pemrosesan komputer secara langsung.

   Namun pendekatan ini memiliki berbagai 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. Cara ini mengabaikan pengendalian sistem dalam pengolahan komputer itu sendiri, sehingga rawan terhadap adanya kelemahan dan kesalahan yang potensial didalamnya.
d. Kemampuan komputer sebagai fasailitas penunjang pelaksanaan audit tidak terpakai.
e. Tidak dapat mencakup keseluruhan maksud dan tujuan penyelenggaraan audit.

2. *Auditing through the computer*

Merupakan suatu pendekatan audit yang berorientasi pada komputer dengan membuka *black box* dan secara langsung berfokus pada operasi pemrosesan dalam sistem komputer. Dengan asumsi bahwa apabila pemrosesan mempunyai pengendalian yang memadai, maka kesalahan dan penyalahgunaan tidak akan terlewat untuk dideteksi, sebagai akibat dari keluaran dapat diterima.

Keuntungan utama dari pendekatan ini adalah 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. Selain itu, dengan memeriksa secara langsung logika pemrosesan dari sistem aplikasi dapat diperkirakan kemampuan sistem dalam menangani perubahan dan kemungkinan kehilangan yang terjadi pada masa yang akan datang.

Kelemahan dari pendekatan ini adalah sebagai berikut :

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*

Pendekatan ini dilakukan dengan menggunakan komputer dan *software* untuk mengotomatisasi prosedur pelaksanaan audit. Pendekatan ini merupakan cara audit yang sangat bermanfaat, khususnya dalam pengujian substantif atas file dan *record* perusahaan. *Software* audit yang digunakan merupakan program komputer auditor untuk mebantu dalam pengujian dan evaluasi kehandalan data, file dan *record* perusahaan.

Keunggulan pendekatan ini adalah :

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

Kelemahan dari pendekatan ini adalah dibutuhkan upaya dan biaya yang relatif besar untuk pengembangannya

2. 4 Tahapan Audit Sistem Informasi

Menurut Hunton (2003:208-212), pada bukunya "Core Concepts of Information Technology Auditing, International Edition". Terdapat tahapan-tahapan yang harus dilakukan dalam melakukan audit antara lain:

1) *Planning*, mendapatkan pemahaman yang lengkap mengenai bisnis perusahaan yang sedang dilakukan audit. Pada proses ini auditor menentukan ruang lingkup dan tujuan pengendalian, tingkat materialitas, dan outsourcing.
2) *Risk Assessment*, menganalisis resiko audit dengan menggunakan *risk-based audit approach* agar pengauditan lebih efisien dan masalah ter-*cover*. Auditor harus memiliki pemahaman mendalam mengenai perusahaan, 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, prosedur audit, dan rincian administratif (perencanaan dan pelaporan).
4) *Gather Evidence*, bertujuan untuk mendapatkan bukti-bukti yang memadai, handal, relevan, dan berguna untuk mencapai sasaran audit secara efektif. Jenis bukti yang sering ditemukan auditor pada kerja lapangan yaitu berupa observasi proses-proses dan keberadaan dari

item fisik seperi pengoperasian komputer atau prosedur *backup* data, bukti dalam bentuk dokumen (seperti program *change logs*, sistem *access logs*, dan tabel otoritas), gambaran dari perusahaan seperi *flowcharts, narratives,* dan kebijakan dan prosedur yang tertulis), serta analisa seperti prosedur CAATs yang dijalankan pada data perusahaan.

5) *Form Conclusion*, mengevaluasi bukti-bukti dan membuat suatu kesimpulan tentang hasil pemeriksaan yang pada akhirnya akan mengarah pada opini audit. Auditor juga akan melaporkan kelemahan dan kelebihan dari sistem.
6) *Deliver Audit Opinion,* informasi umum yang harus ada dalam sebuah laporan audit yaitu:
   a. Nama dari organisasi/ 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 pendistribusian laporan audit

g. Standar-standar dan kriteria yang menjadi dasar auditor untuk melaksanakan pekerjaan audit tersebut

h. Penjelasan rinci mengenai temuan-temuan penting

i. Kesimpulan dari area audit yang dievaluasi, termasuk di dalamnya 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*, melakukan tindak lanjut dengan membuat suatu ketentuan untuk melakukan tindak lanjut bersama dengan perusahaan pada kondisi-kondisi yang dilaporkan atau defisiensi audit yang tidak tercover selama kegiatan audit. Tindak lanjut ini dapat dilakukan dengan menelepon pihak menejemen.

2.5 Teknik Pengumpulan Data

Menurut Sugiyono (2004:130), terdapat beberapa teknik dalam mengumpulkan data, yaitu:

1. Interview (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 / kecil.

2. Kuesioner (Angket)

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

3. Observasi (Pengamatan)

   Observasi mempunyai ciri yang spesifik bila dibandingkan dengan teknik yang lain. Jika wawancara dan kuisioner 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. Observasi dapat berupa :

   a. Analisis catatan (*record analysis*)

      Analisis catatan meliputi catatan historis atau masa kini dan catatan umum atau pribadi, berupa tertulis, dalam bentuk *print-out*.

   b. Analisis kondisi fisik (*physical condition analysis*)

      Merupakan analisis kondisi fisik dari obyek yang diteliti, dalam penelitian ini penulis menganalisa *hardware* dan *software* yang digunakan oleh perusahaan.

c. Analisis proses atau aktivitas (*process or activity analysis*)

Merupakan analisis aktivitas dari obyek yang diteliti, dalam penelitian ini penulis menganalisa proses bisnis yang dilakukan dalam perusahaan

2.6 Pengendalian Internal

2.6.1 Definisi Sistem Pengendalian Internal

Menurut *The Information Sistem Control and Audit Association* (ISACA) yang dikutip oleh Cangemi dan Singleton dalam buku yang berjudul *Managing the Audit Function* (2003:65), pengendalian internal adalah suatu kebijakan, prosedur, praktik-praktik, dan struktur organisasi yang didesain dan dibuat untuk memberikan jaminanpada upaya pencapaian tujuan bisnis yang akan dicapai dan memastikan kejadian-kejadian yang tidak diinginkan akan dicegah, atau dideteksi dan dikoreksi.

Menurut Webber (1999:35), pengendalian adalah suatu sistem untuk mencegah, mendeteksi, dan mengkoreksi kejadian yang timbul saat transaksi dari serangkaian pemrosesan yang tidak terotorisasi secara sah, tidak akurat, tidak lengkap, mengandung redudansi, tidak efektif dan tidak efisien

2.6.2 Tujuan dan Manfaat Sistem Pengendalian Internal

Hall (2001:150) berpendapat bahwa sistem pengendalian internal memiliki empat tujuan utama, yaitu untuk :

1. Mengamankan aktiva organisasi.
2. Memastikan akurasi dan keandalan dari catatan dan informasi akuntansi.
3. Mempromosikan efisiensi operasi perusahaan.
4. Mengukur kesesuaian dengan kebijakan dan prosedur yang telah ditetapkan manajemen.

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.

2.6.3 Macam-macam Pengendalian Internal

Menurut Champlain (2003:28-32) terdapat beberapa kontrol internal yang sangat penting dan harus dilakukan saat melakukan audit sistem informasi, yaitu :

1. *Environmental controls* (kontrol lingkungan)

2. *Physical security controls* (kontrol keamanan fisik)
3. *Logical security controls* (kontrol kemanan logical)
4. *Operation system controls* (kontrol sistem operasi)

Kontrol terhadap lingkungan merupakan kontrol yang paling umum dibandingkan kontrol-kontrol lainnya, yang termasuk dalam kontrol ini adalah kebijakan keamanan sistem informasi, standar, pedoman, stuktur laporan dalam pengolahan sistem informasi (operasi komputer dan pemrograman), dan *license* perangkat lunak dari vendor.

Kontrol keamanan fisik berkaitan dengan perlindungan terhadap perangkat keras komputer, komponen, dan fasilitas-fasilitas yang ada.Meski terbilang kontrol fisik, asuransi atas perangkat keras komputer dan biaya untuk menciptakan kembali atau mengganti program perangkat lunak yang hilang atau rusak dan data juga termasuk di dalamnya.

Kontrol keamanan logis bermanfaat untuk membantu mencegah akses yang tidak sah dan perusakan baik yang disengaja atau tidak disengaja dari program dan data masuk ke dalam perusahaan.Beberapa contohnya adalah kemampuan akses dari *user*, dan mekanisme logging dari *user*.

Kontrol terhadap sistem operasi dirancang untuk membantu memastikan bahwa sistem informasi beroperasi secara efisien dan efektif. Kontrol ini mencakup penyelesaian yang tepat waktu dan

akurat pada tiap proses, distribusi terhadap media output, kinerja prosedur *backup* dan pemulihan, kinerja prosedur pemeliharaan, dokumentasi dan resolusi masalah sistem, dan pemantauan terhadap unit pengolah pusat dan kapasitas penyimpanan data.

2.8 Pengendalian Aplikasi

2.8.1 Definisi Pengendalian Aplikasi

Pengendalian Aplikasi (*Application Controls*) menurut Gondodiyoto (2007:372) adalah, "Sistem pengendalian *intern* komputer pada sistem informasi berbasis teknologi informasi yang berkaitan dengan pekerjaan/ kegiatan/ aplikasi tertentu."

2.8.2 Jenis Pengendalian Aplikasi

Weber (1999:39) membagi pengendalian aplikasi menjadi 6 jenis yaitu:

(1) Pengendalian Batasan (*Boundary Controls*)

Menurut Weber (1999:370), "*The boundary subsistem establishes the interface between the would be user of a computer sistem and the computer sistem itself* ". Inti dari pernyataan tersebut adalah subsistem batasan (*boundary*) membangun suatu hubungan (*interface*) antara pengguna (*user*) komputer dengan sistem komputer itu sendiri melalui suatu tampilan.

(2) Pengendalian Input (*Input Controls*)

Weber (1999:420) berpendapat, "*Components in the input subsistem are responsible for bringing both data and instructionsinto an application controls*". Intinya adalah komponen dalam subsistem *input* bertanggung jawab untuk memasukkan data dan instruksi ke dalam sistem aplikasi. Kedua jenis *input* tersebut harus divalidasi, setiap kesalahan data harus dapat diketahui dan dikontrol sehingga *input* yang dimasukkan akurat, lengkap, dan tepat waktu.

Tiga alasan pentingnya *Input Controls*, yaitu :

(a) Pada sistem informasi kontrol yang besar jumlahnya adalah pada subsistem *input*, sehingga auditor harus memberikan perhatian yang lebih kepada keandalan *input* kontrol yang ada.

(b) Kegiatan subsistem *input* melibatkan jumlah kegiatan yang besar dan rutin dan merupakan kegiatan yang monoton sehingga dapat menyebabkan terjadinya kesalahan.

(c) Subsistem *input* seringkali merupakan target dari *fraud*, banyak kegiatan yang tidak seharusnya dilakukan seperti penambahan, penghapusan, dsb.

(3) Pengendalian *Output* (*Output Controls*)

Gondodiyoto (2007:413) berpendapat bahwa "Pengendalian *output* merupakan pengendalian *intern* untuk mendeteksi jangan sampai informasi yang disajikan tidak akurat, tidak lengkap, tidak

up-to-date (mutakhir) datanya, atau didistribusikan kepada orang-orang yangtidak berwenang".

Berdasarkan sifatnya metode *output controls* terdiri dari tiga jenis, yaitu :

(a) *Preventive Objective*.

Misalnya dengan menggunakan tabel laporan yang terdiri dari jenis laporan, periode laporan, tandaterima konfirmasi, siapa penggunanya, prosedur permintaan laporan.

(b) *Detection Objective*.

Misalnya perlunya dibuat nilai-nilai subtotal dan total yang dapat diperbandingkan untuk mengevaluasi keakurasian laporan.

(c) *Corrective Objective*.

Misalnya tersedianya *help desk* dan *contact person*.

(4) Pengendalian Proses (*Process Controls*)

Menurut Gondodiyoto (2007:401) "Pengendalian proses (*process controls*) adalah pengendalian *intern* untuk mendeteksi jangan sampai data (khususnya data yang sesungguhnya sudah valid) menjadi *error* karena adanya kesalahan proses. Kemungkinan penyebab terjadinya *error* adalah kesalahan logika program, salah rumus, salah urutan program, ketidak terpaduan antara subsistem ataupun kesalahan teknis lainnya".

(5) Pengendalian Komunikasi Aplikasi (Application Communication Control)

Weber (1999:474) berpendapat bahwa "*The communication subsistem is responsible for transporting data among all the othersubsistems within a sistem and for transporting data to or receiving data from another sistem* ". Intinya adalah subsistem komunikasi bertanggung jawab untuk pengiriman data ke subsistem yang lain pada suatu sistem dan untuk pengiriman data ke penerima data dari sistem yang lain.

(6) Pengendalian Basis Data (*Database Controls*)

Weber (1999:563) berpendapat bahwa "*The database subsistem provides function to define, create, modify, delete, and read data inan information sistem*". Intinya adalah bahwa subsistem *database* menyediakan fungsi-fungsi untuk mendefinisikan, menciptakan, memodifikasi, menghapus, dan membaca data di dalam suatu sistem informasi.

2.9 Standarisasi Audit TI

Berikut merupakan beberapa stadarisasi yang digunakan untuk melakukan audit TI menurut Cascarino (2012:47-55):

1. IIA standards, pada tahun 1978 IIA memperkenalkan standar untuk audit practiceof profesional internal yang akan digunakan di seluruh dunia untuk memberikan konsistensi internasional dan sebagai alat ukur untuk

jaminan kualitas audit. Ini terdiri dari lima umum dan 25 standar khusus bersama-sama dengan berbagai pernyataan standar audit. Standar dianggap wajib, sementara non-wajib pedoman juga disertakan. Standar IIA tersebut dimaksudkan untuk membangun tolok ukur untuk pengukuran yang konsisten operasi audit internal. Ini memungkinkan penyatuan audit internal di seluruh dunia dengan meningkatkan praktik audit internal, menyatakan peran, ruang lingkup, kinerja, dan tujuan audit internal, mempromosikan pengakuan profesi audit internal.

2. ISACA standards, tujuan pengendalian untuk informasi dan teknologi terkait sumber daya harus digunakan sebagai sumber bimbingan praktek terbaik (COBIT). Masing-masing diselenggarakan oleh TI proses manajemen, sebagaimana didefinisikan dalam kerangka COBIT. COBIT dimaksudkan untuk digunakan oleh bisnis dan manajemen TI serta IT auditor. Karena itu, memungkinkan pemahaman tujuan bisnis dan komunikasi praktik terbaik dan rekomendasi yang akan dibuat di sekitar acuan standar umum untuk dipahami. COBIT meliputi: tujuan pengendalian, praktek kontrol, pedoman audit, pedoman manajemen.
3. COSO : Internal Control Standards, pada tahun 1992, The American Institute of Certified Public Accountants, The Institute of Internal Auditors, The American Accounting Association, The Institute of Management Accountants, dan The Financial Executives Institute mengeluarkan studi bersama-sama siap berjudul pengendalian internal-suatu kerangka terpadu. Dokumen ini mengidentifikasi tujuan mendasar

dari setiap bisnis atau badan pemerintah. Ini termasuk ekonomi dan efisiensi operasi, pengamanan aset, pencapaian hasil yang diinginkan, keandalan laporan keuangan dan manajemen, dan kepatuhan terhadap hukum dan peraturan.

4. BS 7799 and ISO 17799: IT Security, British Standard (BS) 7799 dan International Standards Organization (ISO) 17799 dikembangkan untuk membantu perusahaan dengan memastikan bahwa, ketika perdagangan elektronik dimasukkan ke dalam, beberapa derajat kepastian mengenai keamanan dan kontrol diimplementasikan di kedua ujung dalam mitra dagang sendiri sistem.
5. Nist, dengan berlalunya Federal Information Security Management Ac (FISMA) tahun 2002, ada ketentuan undang-undang untuk memastikan bahwa lembaga wajib mematuhi Federal Information Processing Standards (FIPS). National Institute of Standards and Technology (NIST) adalah badan federal yang bekerja di bidang teknologi dengan standard an pengukuran teknologi. Computer Security Resource Centre (CSRC), sebuah divisi dari NIST, telah membantu memproduksi kedua buku pedoman tentang keamanan TI serta standar keamanan ganda.

2.10 COBIT 4.1

COBIT merupakan cara atau metode yang dapat ditempuh untuk dapat menganalisa, mengembangkan, mempublikasikan, dan mempromosikan suatu otorisasi. COBIT ini dapat membuat *up-to-date*

suatu sistem perusahaan serta dapat diterima oleh tata kelola TI profesional. Tata kelola TI yang dikontrol dibawah naungan COBIT merupakan tata kelola TI bertaraf internasional.

2.10.1 Kriteria COBIT

Dalam buku yang ditulis oleh ITGI (2007:10-11), untuk memenuhi tujuan bisnis, informasi dibutuhkan untuk memenuhi kriteria kontrol tertentu yang mengacu pada COBIT sebagai persyaratan suatu bisnis untuk informasi. Informasi tersebut harus memiliki tujuh criteria yang didefinisikan sebagai berikut:

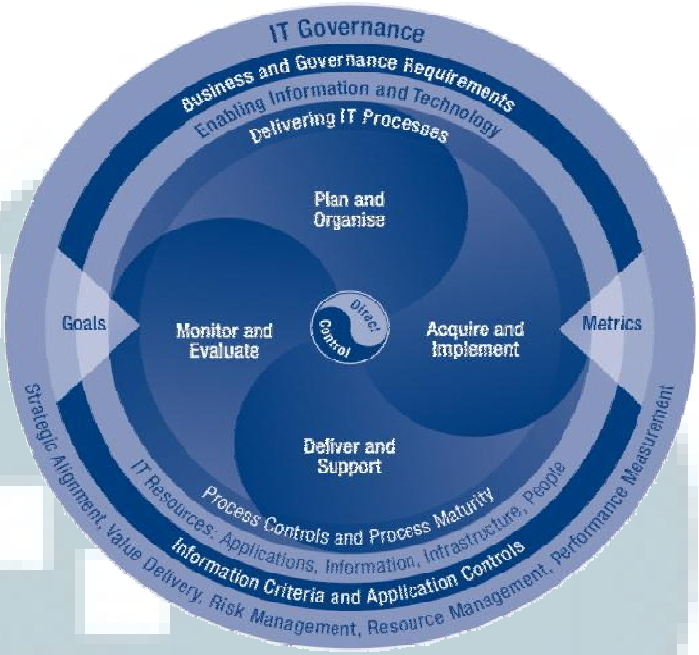
- *Effectiveness* berkaitan dengan informasi yang relevan dan berkaitan dengan proses bisnis serta yang disampaikan dengan cara yang tepat waktu, benar, konsisten dan dapat digunakan.
- *Efficiency* menyangkut penyediaan informasi melalui penggunaan sumber daya yang optimal (paling produktif dan ekonomis).
- *Confidentiality* menyangkut perlindungan informasi sensitif dari pengungkapan yang tidak sah.
- *Integrity* berkaitan dengan keakuratan dan kelengkapan informasi serta validitas sesuai dengan nilai-nilai bisnis dan ekpektasi.
- *Availability* berkaitan dengan informasi yang tersedia pada saat diperlukan oleh proses bisnis yang sekarang dan di masa depan. Hal ini juga menyangkut pengamanan sumber daya yang diperlukan.

- *Compliance* berkaitan dengan mematuhi undang-undang, peraturan, dan kesepakatan kontrak.
- *Reliability* berkaitan dengan penyediaan informasi yang tepat bagi manajemen untuk mengoperasikan entitas dan melaksanakan tanggung jawabnya.

2.10.2 Kerangka Kerja COBIT

Dalam mengatur TI secara efektif, penting untuk mengapresiasikan kegiatan dan risiko dalam TI yang perlu dikelola. Perusahaan biasanya lebih memperhatikan tanggung jawab atas perencanaan, pembangunan, menjalankan, dan memonitor. Dalam standar kerangka kerja COBIT, hal ini telah dibagi menjadi 4 domain penting, yaitu :

- ✓ *Plan and Organise* (PO) - Mengarahkan perusahaan dalam penyampaian solusi (AI) sampai kepada penyampaian pelayanan (DS)
- ✓ *Acquire and Implement* (AI) - Memberikan solusi dan merubahnya menjadi suatu layanan
- ✓ *Deliver and Support* (DS) - Menerima solusi dan mengubahnya agar dapat digunakan untuk penggunaan akhir
- ✓ *Monitor and Evaluate* (ME) - memantau seluruh proses untuk memastikan bahwa arah yang diberikan telah sesuai dijalankan



Gambar 2.1 COBIT Framework

Plan and Organise (PO)

Domain ini meliputi strategi dan taktik yang menyangkut identifikasidari jalan terbaik TI yang dapat memberikan kontribusi pada pencapaian tujuan bisnis. Realisasi visi strategis perlu direncanakan, dikomunikasikan dan dikelola untuk perspektif yang berbeda.ketepatan suatu organisasi serta infrastruktur teknologi harus diletakkan pada wadah yang sama. Domain ini biasanya membahas mengenai pertanyaan manajemen berikut :

a. Apakah TI dan strategi bisnis selaras?
b. Apakah perusahaan mencapai penggunaan optimal dari sumber daya yangdimilikinya?
c. Apakah setiap orang dalam organisasi memahami tujuan TI?
d. Apakah risiko TI dipahami dan dikelola?
e. Apakah kualitas sistem TI cocok dengan kebutuhan bisnis?

Berikut merupakan fokus area tata kelola TI yang dirumuskan ke dalam domain *Plan and Organise* (PO):

Tabel 2.1 Fokus Area Tata Kelola TI Domain PO

Domain	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Plan and Organise							
PO1 Define a strategic IT plan.	P	S					
PO2 Define the information architecture.	S	P	S	P			
PO3 Determine technological direction.	P	P					
PO4 Define the IT processes, organisation and relationships.	P	P					
PO5 Manage the IT investment.	P	P					S
PO6 Communicate management aims and direction.	P					S	
PO7 Manage IT human resources.	P	P					
PO8 Manage quality.	P	P		S			S
PO9 Assess and manage IT risks.	S	S	P	P	P	S	S
PO10 Manage projects.	P	P					

P Primary S Secondary

Berikut ini merupakan kriteria informasi yang dirumuskan ke dalam domain *Plan and Organise* (PO):

Tabel 2.2 Kriteria Informasi Domain PO

Domain	Strategic Alignment	Value Delivery	Risk Management	Resource Management	Performance Measurement
Plan and Organise					
PO1 Define a strategic IT plan.	P		S	S	
PO2 Define the information architecture.	P	S	S	P	
PO3 Determine technological direction.	S	S	S	P	
PO4 Define the IT processes, organisation and relationships.	S		P	P	
PO5 Manage the IT investment.	S	P		S	S
PO6 Communicate management aims and direction.	P		P		
PO7 Manage IT human resources.	P		S	P	S
PO8 Manage quality.	P	S	S		
PO9 Assess and manage IT risks.	P		P		
PO10 Manage projects.	P	S	S	S	S

P Primary S Secondary

Berikut merupakan identifikasi sumber daya TI yang dirumuskan ke dalam domain *Plan and Organise* (PO):

Tabel 2.3 Identifikasi Sumber Daya Domain PO

Domain	Application	Information	Infrastructure	People
Plan and Organise				
PO1 Define a strategic IT plan.	√	√	√	√
PO2 Define the information architecture.	√	√		
PO3 Determine technological direction.	√		√	
PO4 Define the IT processes, organisation				√
PO5 Manage the IT investment.	√		√	√
PO6 Communicate management aims and direction.		√		√
PO7 Manage IT human resources.				√
PO8 Manage quality.	√	√	√	√
PO9 Assess and manage IT risks.	√	√	√	√
PO10 Manage projects.	√		√	√

Acquire and Implement (AI)

Dalam mewujudkan strategi TI, solusi TI perlu untuk diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan dan diintegrasikan ke dalam proses bisnis. Selain itu, domain ini melindungi perubahan dan pemeliharaan sistem yang ada untuk memastikan bahwa solusi tersebut tetap terus memenuhi tujuan bisnis. Domain ini biasanya membahas pertanyaan manajemen berikut:

a. Apakah suatu proyek baru mungkin memberikan solusi yang memenuhi kebutuhan bisnis?
b. Apakah proyek baru mungkin akan dikirimkan tepat waktu dan sesuai anggaran?
c. Akankah sistem baru bekerja dengan baik ketika diimplementasikan?
d. Apakah perubahan dilakukan tanpa mengganggu operasi bisnis saat ini?

Berikut merupakan fokus area tata kelola TI yang dirumuskan ke dalam domain *Acquire and Implement* (AI):

Tabel 2.4 Fokus Area Tata Kelola TI Domain AI

Domain	Strategic Alignment	Value Delivery	Risk Management	Resource Management	Performance Measurement
Acquire and Implement					
AI1 Identify automated solutions.	P	P	S	S	
AI2 Acquire and maintain application software.	P	P	S		
AI3 Acquire and maintain technology infrastructure.				P	
AI4 Enable operation and use.	S	P	S	S	
AI5 Procure IT resources.		S		P	
AI6 Manage changes.		P		S	
AI7 Install and accredit solutions and changes.	S	P	S	S	S

P Primary S Secondary

Berikut ini merupakan kriteria informasi yang dirumuskan ke dalam domain *Acquire and Implement* (AI):

Tabel 2.5 Kriteria Informasi Domain PO

Domain	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Acquire and Implement							
AI1 Identify automated solutions.	P	S					
AI2 Acquire and maintain application software.	P	P		S			S
AI3 Acquire and maintain technology infrastructure.	S	P		S	S		
AI4 Enable operation and use.	P	P		S	S	S	S
AI5 Procure IT resources.	S	P				S	
AI6 Manage changes.	P	P		P	P		S
AI7 Install and accredit solutions and changes.	P	S		S	S		

P Primary S Secondary

Berikut merupakan identifikasi sumber daya TI yang dirumuskan ke dalam domain *Acquire and Implement* (AI):

Tabel 2.6 Identifikasi Sumber Daya Domain AI

Domain	Application	Information	Infrastructure	People
Acquire and Implement				
AI1 Identify automated solutions.	√		√	
AI2 Acquire and maintain application	√			
AI3 Acquire and maintain technology			√	
AI4 Enable operation and use.	√		√	√
AI5 Procure IT resources.	√	√	√	√
AI6 Manage changes.	√	√	√	√
AI7 Install and accredit solutions and	√	√	√	√

Deliver and Support (DS)

Domain ini berkaitan dengan pengiriman aktual dari layanan yang dibutuhkan, yang meliputi pelayanan, pengelolaan keamanan dan kesinambungan, dukungan layanan bagi pengguna, dan pengelolaan data dan fasilitas operasional. Domain ini biasanya membahas pertanyaan manajemen berikut :

a. Apakah layanan TI yang disampaikan sesuai dengan prioritas bisnis?
b. Apakah biaya TI dioptimalkan?
c. Apakah tenaga kerja dapat menggunakan sistem TI secara produktif dan aman?
d. Apakah terdapat tempat yang memadai untuk kerahasiaan, integritas, dan ketersediaan informasi?

Berikut merupakan fokus area tata kelola TI yang dirumuskan ke dalam domain *Deliver and Support* (DS):

Tabel 2.7 Fokus Area Tata Kelola TI Domain DS

Domain	Strategic Alignment	Value Delivery	Risk Management	Resource Management	Performance Measurement
Deliver and Support					
DS1 Define and manage service levels.	P	P		P	P
DS2 Manage third-party services.		P	P	S	S
DS3 Manage performance and capacity.	S	S	S	P	S
DS4 Ensure continuous service.	S	P	P	S	S
DS5 Ensure systems security.			P		
DS6 Identify and allocate costs.		S		P	S
DS7 Educate and train users.	S	P	S	S	
DS8 Manage service desk and incidents.		P			S
DS9 Manage the configuration.		P	S	P	
DS10 Manage problems.		P	S		S
DS11 Manage data.		P	P	P	
DS12 Manage the physical environment.			P	S	
DS13 Manage operations.				P	

P Primary S Secondary

Berikut ini merupakan kriteria informasi yang dirumuskan ke dalam domain *Delivery and Support* (DS):

Tabel 2.8 Kriteria Informasi Domain DS

Domain	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Deliver and Support							
DS1 Define and manage service levels.	P	P	S	S	S	S	S
DS2 Manage third-party services.	P	P	S	S	S	S	S
DS3 Manage performance and capacity.	P	P			S		
DS4 Ensure continuous service.	P	S			P		
DS5 Ensure systems security.			P	P	S	S	S
DS6 Identify and allocate costs.		P					P
DS7 Educate and train users.	P	S					
DS8 Manage service desk and incidents.	P	P					
DS9 Manage the configuration.	P	S			S		S
DS10 Manage problems.	P	P			S		
DS11 Manage data.				P			P
DS12 Manage the physical environment.				P	P		
DS13 Manage operations.	P	P		S	S		

P Primary S Secondary

Berikut merupakan identifikasi sumber daya TI yang dirumuskan ke dalam domain *Deliver and Support* (DS):

Tabel 2.9 Identifikasi Sumber Daya Domain DS

Domain	Application	Information	Infrastructure	People
Deliver and Support				
DS1 Define and manage service levels.	√	√	√	√
DS2 Manage third-party services.	√	√	√	√
DS3 Manage performance and capacity.	√		√	
DS4 Ensure continuous service.	√	√	√	√
DS5 Ensure systems security.	√	√	√	√
DS6 Identify and allocate costs.	√	√	√	√
DS7 Educate and train users.				√
DS8 Manage service desk and incidents.	√			√
DS9 Manage the configuration.	√	√	√	
DS10 Manage problems.	√	√	√	√
DS11 Manage data.		√		
DS12 Manage the physical environment.			√	
DS13 Manage operations.	√	√	√	√

Monitor and Evaluate (ME)

Semua proses TI perlu dinilai secara teratur dari waktu ke waktu untuk kualitas dan pemenuhan persyaratan kontrol. Domain ini membahas kinerja manajemen, pemantauan pengendalian internal, kepatuhan terhadap peraturan dan tata kelola. Domain ini biasanya membahas pertanyaan manajemen berikut:

a. Apakah kinerja TI diukur untuk mendeteksi masalah sebelum terlambat?
b. Apakah manajemen menjamin kontrol internal yang efektif dan efisien?
c. Dapatkah kinerja TI dihubungkan kembali ke tujuan bisnis?
d. Apakah terdapat tempat yang memadai untuk kerahasiaan, integritas, dan ketersediaan informasi?

Berikut merupakan fokus area tata kelola TI yang dirumuskan ke dalam domain *Monitor and Evaluate* (ME):

Tabel 2.10 Fokus Area Tata Kelola TI Domain ME

Domain	Strategic Alignment	Value Delivery	Risk Management	Resource Management	Performance Measurement
Monitor and Evaluate					
ME1 Monitor and evaluate IT performance.	S	S	S	S	P
ME2 Monitor and evaluate internal control.		P	P		
ME3 Ensure compliance with external requirements.	P		P		
ME4 Provide IT governance.	P	P	P	P	P

Berikut ini merupakan kriteria informasi yang dirumuskan ke dalam domain *Monitor and Evaluate* (ME):

Tabel 2.11 Kriteria Informasi Domain ME

Domain	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Monitor and Evaluate							
ME1 Monitor and evaluate IT performance.	P	P	S	S	S	S	S
ME2 Monitor and evaluate internal control.	P	P	S	S	S	S	S
ME3 Ensure compliance with external requirements.						P	S
ME4 Provide IT governance.	P	P	S	S	S	S	S

Berikut merupakan identifikasi sumber daya TI yang dirumuskan ke dalam domain *Monitor and Evaluate* (ME):

Tabel 2.12 Identifikasi Sumber Daya Domain ME

Domain	Application	Information	Infrastructure	People
Monitor and Evaluate				
ME1 Monitor and evaluate IT	√	√	√	√
ME2 Monitor and evaluate internal	√	√	√	√
ME3 Ensure compliance with external	√	√	√	√
ME4 Provide IT governance.	√	√	√	√

Di seluruh empat domain tersebut, COBIT telah mengidentifikasi 34 proses TI yang umumnya digunakan. Sementara kebanyakan perusahaan telah menetapkan suatu rencana, membangun, menjalankan dan memantau tanggung jawab untuk TI, dan sebagian besar memiliki proses kunci yang sama. Jika memiliki struktur proses yang sama maka dapat menerapkan seluruh proses COBIT tersebut.

COBIT memberikan daftar lengkap dari proses yang dapat digunakan untuk memverifikasi kelengkapan kegiatan dan tanggung jawab. Namun, ke 34 proses tersebut tidak harus diberlakukan semuanya, bahkan proses tersebut dapat dikembangkan sendiri atau dapat dikombinasikan seperti yang dipersyaratkan oleh masing-masing perusahaan. Didalam 34 proses tersebut terdapat informasi mengenai bagaimana tujuan dapat diukur, apa kegiatan kunci dan point utama, serta siapa yang bertanggung jawab. Berikut :

1. Plan and Organise

Plan and Organise	
PO1	Define a strategic IT plan.
PO2	Define the information architecture.
PO3	Determine technological direction.
PO4	Define the IT processes, organisation and relationships.
PO5	Manage the IT investment.
PO6	Communicate management aims and direction.
PO7	Manage IT human resources.
PO8	Manage quality.
PO9	Assess and manage IT risks.
PO10	Manage projects.

P01 Define a strategic IT plan

Perencanaan strategis TI diperlukan untuk mengelola dan mengarahkan semua sumber daya TI sejalan dengan prioritas dan strategi bisnis. Bagian TI dan stakeholder bertanggung jawab untuk memastikan bahwa nilai optimal direalisasikan dari portofolio proyek dan layanan. Rencana strategis meningkatkan pemahaman stakeholder akan peluang dan keterbatasan TI, menilai kinerja saat ini, mengidentifikasi kapasitas dan kebutuhan sumber daya manusia, serta menjelaskan tingkat investasi yang dibutuhkan. Strategi bisnis dan prioritas harus tercermin dalam portofolio dan dieksekusi oleh rencana TI, yang menentukan tujuan

singkat, rencana aksi, dan tugas-tugas yang dipahami dan diterima oleh bisnis dan TI.

P02 Define the information architecture

Sistem informasi berfungsi menciptakan dan secara teratur memperbarui model informasi bisnis dan mendefinisikan sistem yang sesuai untuk mengoptimalkan penggunaan informasi ini. Hal ini meliputi pengembangan kamus data perusahaan dengan organisasi, aturan data sintaks, klasifikasi skema data dan tingkat keamanan. Proses ini meningkatkan kualitas pengambilan keputusan manajemen dengan memastikan bahwa informasi yang disediakan dapat dipercaya dan aman, serta memungkinkan sistem informasi sumber daya rasionalisasi untuk tepat sesuai dengan strategi bisnis. Proses ini juga diperlukan untuk meningkatkan akuntabilitas untuk integritas dan keamanan data untuk meningkatkan efektivitas kontrol berbagi informasi di seluruh aplikasi dan entitas.

P03 Determine technological direction

Informasi layanan berfungsi menentukan arah teknologi untuk mendukung bisnis. Hal ini membutuhkan penciptaan rencana infrastruktur teknologi dan dasar arsitektur yang ditetapkan dan dikelola secara jelas dan realistis tentang teknologi apa yang dapat ditawarkan dalam hal produk, layanan dan mekanisme pengiriman. Rencananya secara teratur diperbarui dan mencakup aspek-aspek seperti arsitektur sistem, arah teknologi, rencana akuisisi, standar, strategi migrasi dan kontingensi. Ini

memungkinkan respon menjadi tepat waktu terhadap perubahan dalam lingkungan yang kompetitif, skala ekonomi untuk staf sistem informasi dan investasi, serta sebagai interoperabilitas peningkatan platform dan aplikasi.

P04 Define the IT processes, organisation, and relationships

Sebuah organisasi TI didefinisikan dengan mempertimbangkan persyaratan untuk staf, keterampilan, fungsi, akuntabilitas, otoritas, peran dan tanggung jawab, serta pengawasan. Organisasi ini tertanam ke dalam kerangka proses TI yang menjamin transparansi dan kontrol serta keterlibatan eksekutif senior dan manajemen bisnis. Sebuah komite strategi menjamin pengawasan dewan TI, dan pengaruh komite di mana bisnis dan TI berpartisipasi menentukan prioritas sumber daya TI sesuai dengan kebutuhan bisnis.

Proses, kebijakan dan prosedur administratif menjadi alat untuk semua fungsi, dengan perhatian khusus untuk mengontrol, jaminan kualitas, manajemen resiko, keamanan informasi, data dan sistem kepemilikan, dan pemisahan tugas. Untuk memastikan dukungan yang tepat waktu dari kebutuhan bisnis, TI terlibat dalam proses pengambilan keputusan yang relevan.

P05 Manage the IT investment

Sebuah framework yang ditetapkan dan dipelihara untuk mengelola ketersediaan program investasi dan yang meliputi biaya, manfaat, prioritas anggaran, proses penganggaran formal dan manajemen terhadap anggaran.

Stakeholder dikonsultasikan untuk mengidentifikasi dan mengendalikan total biaya dan manfaat dalam konteks rencana TI strategis dan taktis, dan memulai tindakan korektif jika diperlukan. Proses menumbuhkan kemitraan antara TI dan pemangku kepentingan bisnis, memungkinkan penggunaan yang efektif dan efisien dari sumber daya TI, dan menyediakan transparansi dan akuntabilitas ke dalam total biaya kepemilikan (TCO), realisasi keuntungan bisnis dari investasi TI.

P06 Communicate management aims and direction

Manajemen mengembangkan suatu kerangka pengendalian, pendefinisian, dan pengkomunikasian kebijakan perusahaan IT. Sebuah program komunikasi berkelanjutan dilaksanakan untuk mengartikulasikan misi, tujuan layanan, kebijakan dan prosedur, dll, disetujui dan didukung oleh manajemen. Komunikasi mendukung pencapaian tujuan TI dan memastikan kesadaran dan pemahaman tentang bisnis dan risiko TI, tujuan dan arah. Proses tersebut memastikan kepatuhan terhadap hukum dan peraturan.

P07 Manage IT human resources

Tenaga kerja yang kompeten diperoleh dan dipertahankan untuk penciptaan dan pengiriman layanan TI untuk bisnis. Hal ini dicapai dengan ditetapkan dan disepakatinya praktik mendukung perekrutan, pelatihan, evaluasi kinerja, mempromosikan dan mengakhiri. Proses ini sangat penting, karena tenaga kerja merupakan aset penting, dan tata kelola serta

pengendalian internal sangat bergantung pada motivasi dan kompetensi personil

P08 Manage quality

QMS (*Quality Management System*) dikembangkan dan dipelihara meliputi pembangunan terbukti dan proses akuisisi dan standar. Ini diaktifkan dengan perencanaan, pelaksanaan dan pemeliharaan QMS dengan memberikan persyaratan mutu yang jelas, prosedur dan kebijakan. Persyaratan mutu dinyatakan dan dikomunikasikan dalam indikator kuantitatif dan dapat dicapai. Perbaikan terus-menerus dicapai dengan pemantauan, analisis dan bertindak atas penyimpangan, dan mengkomunikasikan hasilnya kepada para stakeholder. Manajemen mutu sangat penting untuk memastikan bahwa TI memberikan nilai bagi perbaikan bisnis yang berkesinambungan dan transparansi bagi para pemangku kepentingan.

P09 Assess and manage IT risks

Kerangka ini harus dibuat dan dipelihara. Kerangka kerja ini mendokumentasikan tingkat umum. Dampak potensial pada tujuan dari organisasi yang disebabkan oleh suatu peristiwa yang tidak direncanakan diidentifikasi, dianalisa dan dinilai. Risiko strategi mitigasi yang diadopsi untuk meminimalkan risiko residual ke tingkat yang dapat diterima. Hasil dari penilaian tersebut dapat dimengerti kepada para stakeholder dan dinyatakan dalam istilah keuangan, untuk memungkinkan para stakeholder untuk menyelaraskan risiko ke tingkat yang dapat diterima.

PO10 Manage projects

Sebuah program dan kerangka kerja manajemen proyek untuk mengatur semua proyek TI. Kerangka kerja ini menjamin prioritas yang benar dan koordinasi dari semua proyek. Kerangka kerja ini termasuk master plan, penugasan sumber daya, pengiriman, persetujuan oleh pengguna, pendekatan bertahap untuk pengiriman, QA, rencana uji formal, dan pengujian dan pasca-pelaksanaan review setelah instalasi untuk memastikan proyek manajemen risiko dan pengiriman nilai bisnis. Pendekatan ini mengurangi risiko biaya tak terduga dan pembatalan proyek, meningkatkan komunikasi dan keterlibatan pengguna bisnis dan pengguna akhir, memastikan nilai dan kualitas deliverable proyek, dan memaksimalkan kontribusi mereka terhadap investasi IT program

2. Acquire and Implement

Acquire and Implement	
AI1	Identify automated solutions.
AI2	Acquire and maintain application software.
AI3	Acquire and maintain technology infrastructure.
AI4	Enable operation and use.
AI5	Procure IT resources.
AI6	Manage changes.
AI7	Install and accredit solutions and changes.

AI1 Identify automated solutions

Kebutuhan untuk aplikasi baru memerlukan analisis sebelum adanya akuisisi atau penciptaan untuk memastikan bahwa kebutuhan bisnis puas dalam pendekatan yang efektif dan efisien. Proses ini meliputi definisi kebutuhan, pertimbangan sumber alternatif, review kelayakan teknologi dan ekonomi, pelaksanaan analisis risiko dan analisis biaya-manfaat, dan kesimpulan atas keputusan akhir untuk 'membuat' atau 'membeli'. Semua langkah memungkinkan organisasi untuk meminimalkan biaya untuk memperoleh dan menerapkan solusi sementara memastikan bahwa ada kemungkinan untuk mencapai tujuan.

AI2 Acquire and maintain application software

Aplikasi yang dibuat tersedia sesuai dengan kebutuhan bisnis. Proses ini meliputi desain aplikasi, memasukan kontrol ke aplikasi sesuai persyaratan keamanan, dan pengembangan konfigurasi sesuai dengan standar. Hal ini memungkinkan organisasi untuk benar mendukung operasi bisnis dengan aplikasi otomatis yang benar.

AI3 Acquire and maintain technology infrastructure

Organisasi memiliki proses untuk pelaksanaan, akuisisi dan upgrade dari infrastruktur teknologi. Ini membutuhkan pendekatan yang direncanakan untuk diakuisisi, pemeliharaan dan perlindungan infrastruktur sejalan dengan yang telah disepakati strategi teknologi dan penyediaan lingkungan pengembangan dan pengujian. Hal ini memastikan

bahwa ada dukungan teknologi yang sedang berlangsung untuk aplikasi bisnis

AI4 Enable operation and use

Tersedianya pengetahuan tentang sistem baru. Proses ini membutuhkan pembuatan dokumentasi dan manual bagi pengguna dan bagian IT. Penyediaan pelatihan untuk memastikan penggunaan yang tepat dan pengoperasian aplikasi dan infrastruktur.

AI5 Procure IT resources

Sumber daya TI, termasuk SDM, *hardware*, software dan jasa, perlu diperoleh. Hal ini memerlukan definisi dan penegakan prosedur pengadaan, pemilihan vendor, setup pengaturan kontrak, dan akuisisi itu sendiri. Memastikan bahwa organisasi memiliki semua yang diperlukan sumber daya TI secara tepat waktu dan hemat biaya.

AI6 Manage changes

Semua perubahan, termasuk perawatan darurat dan patch yang berkaitan dengan infrastruktur dan aplikasi dalam lingkungan produksi secara resmi dikelola dengan cara yang terkendali. Perubahan (termasuk parameter prosedur, proses, sistem dan layanan) akan dicatat, dinilai dan diberlakukan sebelum pelaksanaan dan ditinjau terhadap hasil yang direncanakan menyusul implementasi.

AI7 Install and accredit solutions and changes

Sistem baru perlu dibuat operasional setelah pembangunan selesai. Hal ini membutuhkan pengujian yang tepat dalam lingkungan khusus

dengan data uji yang relevan, instruksi peluncuran dan migrasi, perencanaan rilis dan promosi yang sebenarnya untuk produksi, dan kajian pasca implementasi. Hal ini menjamin bahwa sistem operasional sejalan dengan yang disepakati.

3. Deliver and Support

Deliver and Support	
DS1	Define and manage service levels.
DS2	Manage third-party services.
DS3	Manage performance and capacity.
DS4	Ensure continuous service.
DS5	Ensure systems security.
DS6	Identify and allocate costs.
DS7	Educate and train *user*s.
DS8	Manage service desk and incidents.
DS9	Manage the configuration.
DS10	Manage problems.
DS11	Manage data.
DS12	Manage the physical environment.
DS13	Manage operations.

DS1 Define and manage service levels

Komunikasi yang efektif antara TI dan bisnis manajemen pelanggan mengenai layanan yang dibutuhkan diaktifkan oleh dokumentasi definisi dan kesepakatan layanan TI dan tingkat layanan. Proses ini juga mencakup pemantauan dan pelaporan yang tepat bagi pemegang saham atas pencapaian tingkat layanan. Proses ini memungkinkan keselarasan antara layanan TI dan kebutuhan bisnis yang terkait.

DS2 Manage third-party services

Kebutuhan untuk memastikan bahwa layanan yang diberikan oleh pihak ketiga (pemasok, vendor dan mitra) memenuhi kebutuhan bisnis memerlukan proses manajemen yang efektif. Proses ini dilakukan dengan mendefinisikan secara jelas peran, tanggung jawab dan harapan pihak ketiga, perjanjian serta meninjau dan pemantauan perjanjian tersebut untuk efektivitas dan kepatuhan. Manajemen yang efektif dari layanan pihak ketiga meminimalkan risiko bisnis yang terkait dengan non-performing pemasok.

DS3 Manage performance and capacity

Kebutuhan untuk mengelola kinerja dan kapasitas sumber daya TI membutuhkan proses untuk secara berkala meninjau kinerja dan kapasitas sumber daya TI. Proses ini meliputi peramalan kebutuhan masa depan berdasarkan beban kerja serta penyimpanan dan persyaratan kontingensi.

Proses ini memberikan jaminan bahwa informasi sumber daya yang mendukung kebutuhan bisnis yang terus tersedia.

DS4 Ensure continuous service

Kebutuhan untuk menyediakan layanan TI terus menerus memerlukan pengembangan, pemeliharaan dan pengujian rencana yang berkesinambungan, memanfaatkan penyimpanan cadangan offsite dan memberikan pelatihan kelangsungan rencana periodik. Sebuah proses pelayanan yang efektif terus menerus meminimalkan kemungkinan dan dampak dari gangguan layanan TI.

DS5 Ensure systems security

Kebutuhan untuk menjaga integritas informasi dan melindungi aset TI membutuhkan proses manajemen keamanan. Proses ini meliputi membangun dan mempertahankan peran keamanan TI dan Tanggung Jawab, kebijakan, standar, dan prosedur. Keamanan manajemen juga mencakup pemantauan keamanan dan pengujian berkala, melaksanakan tindakan korektif untuk insiden. Manajemen keamanan yang efektif melindungi semua aset TI untuk meminimalkan dampak bisnis rentannya keamanan dan insiden.

DS6 Identify and allocate costs

Kebutuhan sistem yang adil dan merata mengalokasikan biaya TI untuk bisnis memerlukan pengukuran akurat dari biaya TI dan kesepakatan dengan pengguna bisnis pada alokasi yang adil. Proses ini meliputi membangun dan mengoperasikan sebuah sistem untuk menangkap,

mengalokasikan dan melaporkan biaya TI kepada pengguna jasa. Sebuah sistem yang adil memungkinkan bisnis untuk membuat keputusan yang lebih tepat tentang penggunaan layanan TI.

DS7 Educate and train *user*s

Pendidikan yang efektif dari semua pengguna sistem TI, termasuk dalam IT, membutuhkan identifikasi kebutuhan pelatihan dari masing-masing kelompok pengguna. Selain mengidentifikasi kebutuhan, proses ini termasuk mendefinisikan dan melaksanakan strategi untuk pelatihan yang efektif dan mengukur hasilnya. Sebuah program pelatihan yang efektif meningkatkan penggunaan teknologi yang efektif dengan mengurangi kesalahan pengguna, meningkatkan produktivitas dan meningkatkan kepatuhan dengan kontrol utama, seperti langkah-langkah keamanan pengguna.

DS8 Manage service desk and incidents

Respon yang tepat waktu dan efektif untuk permintaan pengguna dan memecahkan masalah membutuhkan layanan yang dirancang dengan baik dan pelaksanaan yang lebih baik serta proses manajemen insiden. Proses ini termasuk menyiapkan fungsi pelayanan meja dengan pendaftaran, trend insiden, eskalasi dan analisis akar penyebab, dan resolusi. Manfaat bisnis meliputi peningkatan produktivitas melalui resolusi cepat permintaan pengguna. Selain itu, bisnis dapat mengatasi akar penyebab melalui pelaporan yang efektif.

DS9 Manage the configuration

Memastikan integritas konfigurasi *hardware* dan software memerlukan pembentukan dan pemeliharaan suatu repositori konfigurasi yang akurat dan lengkap. Proses ini termasuk mengumpulkan informasi konfigurasi awal, pembangunan dasar, memverifikasi dan informasi audit konfigurasi, dan memperbarui repositori konfigurasi yang diperlukan. Manajemen konfigurasi yang efektif memfasilitasi ketersediaan sistem yang lebih besar, meminimalkan masalah produksi dan menyelesaikan masalah lebih cepat.

DS10 Manage problems

Masalah manajemen yang efektif memerlukan identifikasi dan klasifikasi masalah, analisis akar penyebab dan resolusi masalah. Proses manajemen masalah juga mencakup perumusan rekomendasi untuk perbaikan, pemeliharaan catatan masalah dan penelaahan tindakan korektif. Sebuah proses masalah manajemen yang efektif memaksimalkan ketersediaan sistem, meningkatkan tingkat layanan, mengurangi biaya, dan meningkatkan kenyamanan dan kepuasan pelanggan.

DS11 Manage data

Manajemen data yang efektif memerlukan identifikasi kebutuhan data. Proses manajemen data juga mencakup pembentukan prosedur yang efektif untuk mengelola perpustakaan media, backup dan pemulihan data, dan pembuangan yang tepat dari media. Pengelolaan data yang efektif

membantu memastikan kualitas, ketepatan waktu dan ketersediaan data bisnis.

DS12 Manage the physical environment

Perlindungan untuk peralatan komputer dan personil membutuhkan fasilitas fisik yang dirancang dengan baik dan dikelola dengan baik juga. Proses pengelolaan lingkungan fisik meliputi mendefinisikan persyaratan situs fisik, memilih fasilitas yang tepat, dan merancang proses yang efektif untuk memantau faktor lingkungan dan mengelola akses fisik. Manajemen yang efektif dari lingkungan fisik mengurangi gangguan bisnis dari kerusakan peralatan komputer dan personil.

DS13 Manage operations

Pengolahan data yang lengkap dan akurat membutuhkan manajemen yang efektif dari prosedur pengolahan data dan pemeliharaan perangkat keras. Proses ini termasuk menentukan kebijakan operasional dan prosedur manajemen yang efektif dijadwalkan, melindungi output yang sensitif, pemantauan kinerja infrastruktur dan memastikan pemeliharaan preventif perangkat keras. Manajemen operasi yang efektif membantu menjaga integritas data dan mengurangi penundaan bisnis dan biaya operasional TI.

4. Monitor and Evaluate

Monitor and Evaluate
ME1 Monitor and evaluate IT performance.

ME2	Monitor and evaluate internal control.
ME3	Ensure compliance with external requirements.
ME4	Provide IT governance.

ME1 Monitor and evaluate IT performance

Kinerja manajemen TI yang efektif membutuhkan proses pemantauan. Proses ini mencakup indikator kinerja, mendefinisikan hal-hal yang relevan, pelaporan yang sistematis dan tepat waktu, dan cepat bertindak atas penyimpangan. Pemantauan diperlukan untuk memastikan bahwa hal yang benar dilakukan dan sejalan dengan arah dan kebijakan yang telah ditetapkan.

ME2 Monitor and evaluate internal control

Membentuk program pengendalian internal yang efektif untuk TI membutuhkan proses monitoring yang jelas. Proses ini meliputi pemantauan dan pelaporan kontrol, ulsan dari hasil penilaian diri dan pihak ketiga. Manfaat utama dari pemantauan pengendalian internal adalah untuk memberikan keyakinan yang berkaitan dengan operasi yang efektif dan efisien serta kepatuhan terhadap hukum dan peraturan yang berlaku.

ME3 Ensure compliance with external requirements

Pengawasan kepatuhan yang efektif mengharuskan pembentukan proses review untuk memastikan kepatuhan terhadap undang-undang dan peraturan persyaratan kontrak. Proses ini meliputi identifikasi persyaratan kepatuhan, mengoptimalkan dan mengevaluasi respon, memperoleh

jaminan bahwa persyaratan telah dipenuhi dan pada akhirnya, mengintegrasikan pelaporan kepatuhan TI dengan bisnis yang tersisa.

ME4 Provide IT governance

Membangun kerangka kerja tata kelola yang efektif termasuk menentukan struktur organisasi, proses, kepemimpinan, peran dan tanggung jawab. Tujuannya adalah untuk memastikan bahwa keselarasan perusahaan investasi TI disampaikan sesuai dengan strategi perusahaan dan tujuan.